FortiGate NGFW to FortiSASE SPA Hub Conversion Using Fabric Overlay Orchestrator Deployment Guide

FortiSASE

DEFINE / DESIGN / DEPLOY / DEMO

Table of Contents

Change log 4
Deployment overview 5
Intended audience 7
About this guide 7
Design concept and considerations 7
FortiGate NGFW 7
FortiSASE SPA hub versus SD-WAN hub 7
Fabric Overlay Orchestrator 8
Network restrictions 9
Product prerequisites 9
Deployment plan 9
Deployment procedures 10
Provisioning your FortiSASE instance 10
Converting FortiGate NGFW to a FortiSASE SPA hub using FortiOS Fabric Overlay Orchestrator 10
General steps 11
Policy creation 11
Configuring a root FortiGate using the Fabric Overlay Orchestrator 12
Configuring a downstream FortiGate using the Fabric Overlay Orchestrator 14
Configuring an overlay on spoke for additional incoming interface on hub (if applicable) 16
Verifying firewall policies on the hub FortiGate 17
Verifying settings 18
Configuring SPA to the FortiGate SPA hub in FortiSASE Secure Private Access 25
Configuration workflow 25
BGP routing design 25
Configuring network configuration 26
Configuring a new service connection 30
Viewing health and VPN tunnel status 35
Editing SLA thresholds 36
Updating service connection priorities 37
Deleting a hub configuration 38
Configuring SPA using the REST API 39

Monitoring private access hubs 39
Configuring a private access policy for client-to-server traffic 40
Configuring a private access policy for server-to-client traffic 43
Configuring a private access security profile 45
Configuring ZTNA tags in private access policies 45
Configuring DNS Settings 53
Split DNS Rules 54
Verifying IPsec VPN tunnels on the FortiGate hub 58
Verifying BGP routing on the FortiGate hub 59
Testing private access connectivity to FortiGate hub network from remote VPN users and edge devices 60
Testing private access connectivity to FortiGate hub network from remote SWG users 60
Testing private access connectivity from FortiGate hub network to remote VPN users 60
Verifying private access traffic in FortiSASE portal 61
Verifying private access traffic from hubs 63
Verifying private access hub status and location using the asset map 63
More information 65
Appendix A: Documentation references 65
Feature documentation 65
4-D resources: SASE 65
Appendix C - Converting FortiGate NGFW configured using FortiOS GUI to a FortiSASE SPA hub without using the Fabric Overlay Orchestrator 65
IPsec VPN configuration 66
Tunnel interface configuration 70
Loopback interface configuration 71
Firewall policy configuration 72
BGP configuration 74

Change log

Date	Change description
2025-05-09	Initial release.
2025-05-13	Updated: • Configuring SPA to the FortiGate SPA hub in FortiSASE Secure Private Access on page 25 • Configuring network configuration on page 26
2025-05-14	Updated: • Configuring network configuration on page 26 • Configuring a new service connection on page 30
2025-05-16	Updated: • Configuring SPA to the FortiGate SPA hub in FortiSASE Secure Private Access on page 25 • Configuring network configuration on page 26 • Configuring a new service connection on page 30 • Editing SLA thresholds on page 36 • Updating service connection priorities on page 37
2025-05-20	Added: • Configuring a private access policy for client-to-server traffic on page 40 • Configuring a private access policy for server-to-client traffic on page 43

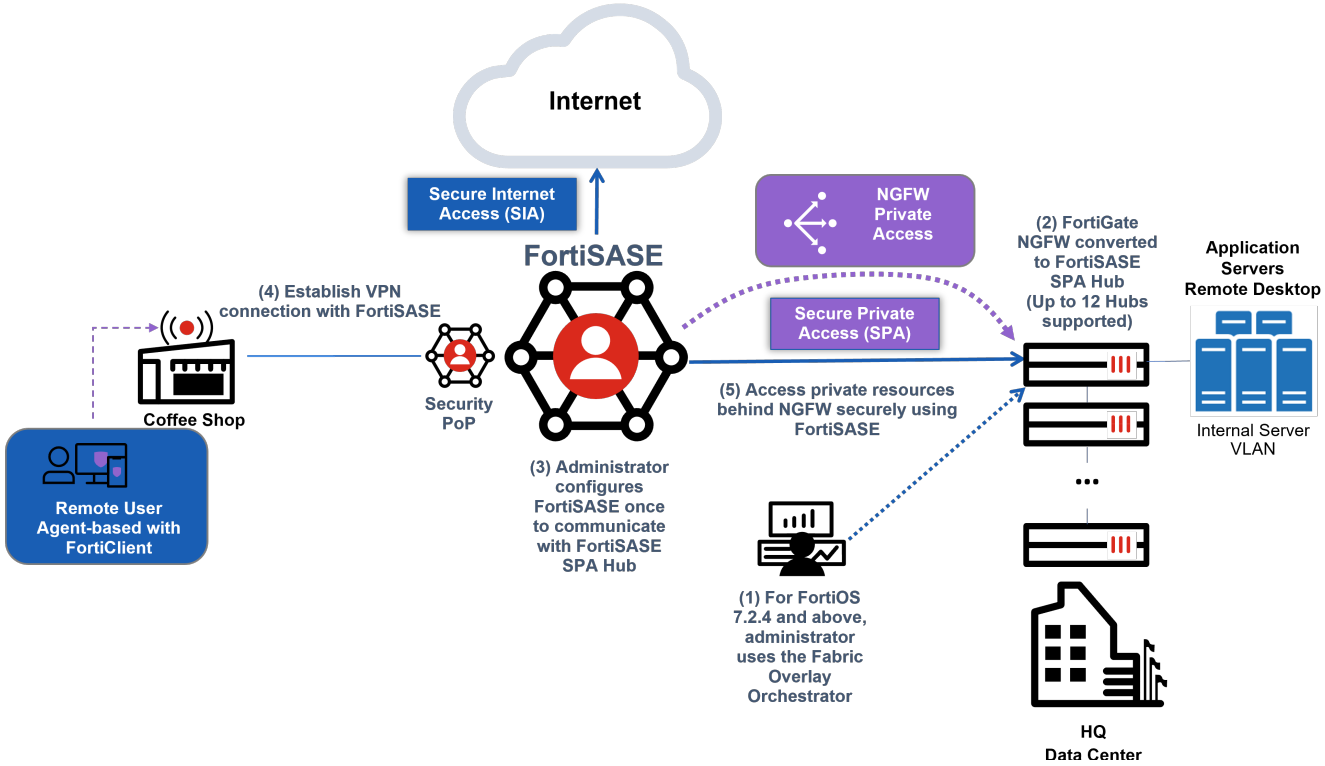
Deployment overview

Organizations that have resources behind a newly deployed FortiGate next generation firewall (NGFW) standalone site or behind a newly deployed FortiGate NGFW in a data center and are not configured with SD-WAN enabled can provide their FortiSASE remote users with access to private resources.

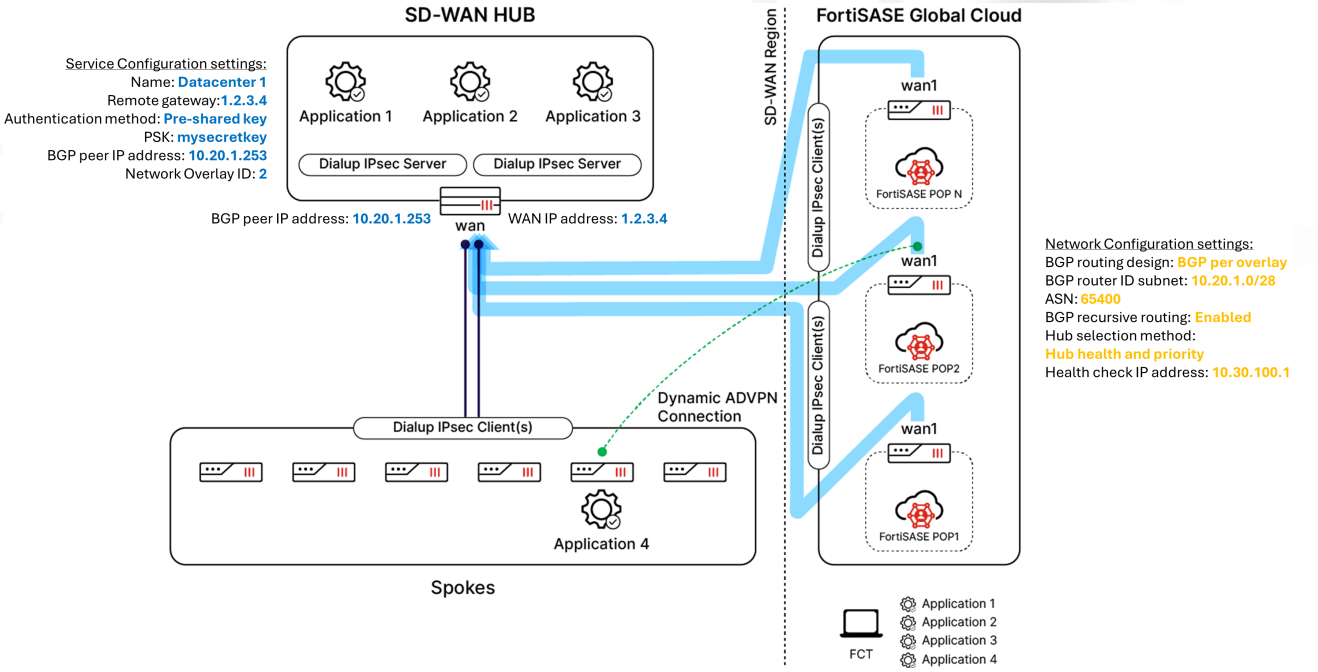
Scenarios involving a FortiGate NGFW converted to a FortiSASE secure private access (SPA) hub or involving an existing FortiGate SD-WAN hub allow broader and seamless access to privately hosted TCP- and UDP-based applications.

In the NGFW SPA use case, you must first convert the newly deployed NGFW to a FortiSASE SPA hub. Starting in FortiOS 7.2.4, you can accomplish this using Fabric Overlay Orchestrator. After configuring FortiSASE to communicate with this hub, the FortiSASE security points-of-presence (PoPs) act as spokes to this hub, relying on IPsec VPN overlays and iBGP to secure and route traffic between PoPs and the networks behind the organization's NGFW.

A typical topology for deploying this example design is as follows:


Internet
Secure Internet Access (SIA)
FortiSASE
NGFW Private Access
(2) FortiGate NGFW converted to FortiSASE SPA Hub (Up to 12 Hubs supported)
Application Servers Remote Desktop
(4) Establish VPN connection with FortiSASE
Secure Private Access (SPA)
Coffee Shop
Security PoP
(5) Access private resources behind NGFW securely using FortiSASE
Internal Server VLAN
Remote User Agent-based with FortiClient
(3) Administrator configures FortiSASE once to communicate with FortiSASE SPA Hub
(1) For FortiOS 7.2.4 and above, administrator uses the Fabric Overlay Orchestrator
HQ Data Center

FortiSASE PoPs and the organization's FortiGate hubs form a traditional hub-and-spoke topology that supports the Fortinet autodiscovery VPN (ADVPN) configuration. ADVPN is an IPsec technology that allows a traditional hub-and-spoke VPN's spokes to establish dynamic, on-demand, direct tunnels, known as shortcut tunnels, between each other to avoid routing through the topology's hub device.



FortiSASE remote users may access private resources behind FortiGate hub(s) directly through FortiSASE to hub(s) IPsec tunnels. If a private resource is behind an organization's spoke device, they may connect directly to that resource through an on-demand, direct, and dynamic ADVPN tunnel.

The SPA use cases with FortiGate hubs allow traffic flow in the following directions:

From...	To...
Remote VPN users	FortiGate hubs (or spokes connected to hubs)
FortiGate hubs (or spokes connected to hubs)	Remote VPN users

FortiSASE supports these main routing design methods:

- BGP per overlay (default)
- BGP on loopback

This deployment guide only covers the FortiGate configuration for the BGP per overlay routing design.

This deployment guide describes how to configure a new FortiGate NGFW deployment to convert it to become a FortiSASE SPA hub and covers the cases when the newly deployed FortiGate NGFW is configured using Fabric Overlay Orchestrator in FortiOS 7.2.4 and later. After performing the conversion steps and subsequent FortiSASE configuration steps, FortiSASE remote users can privately access internal networks behind these deployments.

For deployment details for the existing SD-WAN SPA use case, see the 4-D FortiSASE SPA with a FortiGate SD-WAN Deployment Guide instead of this guide.

For a list of product prerequisites, see SPA using a FortiSASE SPA hub with Fabric overlay orchestrator.

Intended audience

Midlevel network and security administrators of FortiGate NGFW devices in companies of all sizes and verticals should find this guide helpful. A working knowledge of FortiOS, FortiGate, and FortiManager configuration and the Fortinet Security Fabric is helpful.

About this guide

This deployment guide describes the steps involved in deploying a specific architecture for the FortiSASE SPA use case using a FortiGate NGFW converted to a FortiSASE SPA hub.

Readers should first evaluate their environment to determine whether the architecture outlined in this guide suits them. Reviewing the reference architecture guide(s), such as the FortiSASE Architecture Guide, is advisable if readers are still in the process of selecting the right architecture. See also the FortiSASE Concept Guide.

This deployment guide presents one of possibly many ways to deploy the solution. It may also omit specific steps where readers must make design decisions to further configure their devices. Reviewing supplementary material found on the Fortinet Document Library in product administration guides, example guides, cookbooks, release notes, and other documents is recommended, where appropriate.

Design concept and considerations

FortiGate NGFW

The FortiGate in the standalone next generation firewall (NGFW) topology is typically used by customers with a single FortiGate deployed on-premise to protect their site or with a single FortiGate deployed on-premise per site when multiple sites are involved. The design goals for deploying a FortiGate NGFW device are to use it for NGFW protection including antivirus, web filtering, intrusion prevention system (IPS), and application control features, and for LAN segmentation. Typically, a FortiGate NGFW has not yet been configured with advanced features such as SD-WAN, zero trust network access, or FortiSASE.

This guide covers the cases when the newly deployed FortiGate NGFW is configured using the FortiOS CLI or GUI, or managed using FortiManager.

This guide assumes a newly deployed FortiGate NGFW, which means that the device does not contain any existing routing or firewall policies to reconfigured.

FortiSASE SPA hub versus SD-WAN hub

This guide describes steps required to configure the FortiGate NGFW as a FortiSASE SPA hub. A FortiSASE SPA hub allows the FortiSASE Security Points of Presence (PoPs) to connect to the hub as spokes. Essentially, the FortiGate becomes an IPsec Auto-Discovery VPN (ADVPN) hub in a hub-and-spoke topology, and for most deployments, this configuration will be sufficient to provide FortiSASE remote users with secure private access to internal resources behind the FortiGate NGFW.

SD-WAN uses ADVPN for its VPN overlay. In some deployments, administrators may prefer configuring their FortiGate NGFW as an SD-WAN hub instead of just as an ADVPN hub. For these deployments, administrators require additional configuration of SD-WAN performance SLAs and SD-WAN rules using the FortiOS CLI or GUI, or use

FortiManager to ensure their FortiGate NGFW become fully SD-WAN enabled. These configuration changes to convert an ADVPN hub to an SD-WAN hub are outside of the scope of this guide.

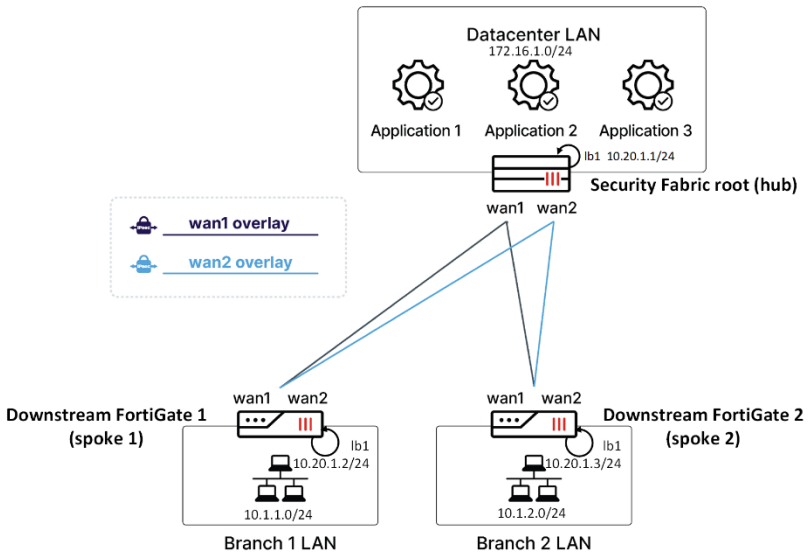
For more details on SD-WAN configuration, then please refer to Performance SLA and SD-WAN Rules sections of the FortiOS Admin Guide.

Fabric Overlay Orchestrator

FortiOS 7.2.4 and above includes a Fabric Overlay Orchestrator feature, which is an easy-to-use GUI wizard that simplifies the process of configuring a self-orchestrated SD-WAN overlay within a single Security Fabric. This feature is self-orchestrated since no additional tool or device aside from the FortiGates themselves is required to orchestrate this configuration. An SD-WAN overlay configuration consists of IPsec and BGP configuration settings.

Currently, the Fabric Overlay Orchestrator supports a single hub architecture and builds upon an existing Security Fabric configuration. This feature configures the root FortiGate as the SD-WAN overlay hub and configures the downstream FortiGates, namely, first-level children from the root, as the spokes.

The Fabric Overlay Orchestrator supports configuring an overlay for the following example hub-and-spoke topology using ADVPN and a single hub as depicted below:



The above network topology corresponds to the single datacenter (active-passive gateway) design using the IPsec overlay design of one-to-one overlay mapping per underlay. For further details on these topics, see the SD-WAN Architectures for Enterprises design guide.

In the hub-and-spoke topology above, the datacenter FortiGate (or the Root FortiGate in the Security Fabric) is the hub and the branch FortiGates (or the Downstream FortiGates in the Security Fabric) are the spokes. Each FortiGate has a distinct LAN subnet defined and has a loopback interface, lb1, with an IP address within the 10.20.1.0/24 subnet.

The Fabric Overlay Orchestrator creates loopbacks to act as health check servers that are always up, and which can be accessed by adjacent fabric devices. When configured with the policy creation options of automatic or health check on the hub, the Fabric Overlay Orchestrator configures performance SLA from the hub to the health check servers on 10.20.1.2 and 10.20.1.3 corresponding to Spoke 1 and Spoke 2 FortiGate devices, respectively. Likewise, the Fabric Overlay Orchestrator when run on each spoke creates a performance SLA to the Hub using its loopback address 10.20.1.1.

Instead of using loopbacks, any business-critical applications and resources connected to the LAN of each device can be used as health check servers for performance SLAs.

Network restrictions

As some IP addresses ranges are reserved for FortiSASE internal usage, note the network restrictions in Network restrictions.

Product prerequisites

For a list of product prerequisites, see SPA using a FortiSASE SPA hub using the FortiOS Fabric Overlay Orchestrator feature in the FortiSASE Release Notes.

Deployment plan

This outlines the major steps to deploy this solution. Go to Deployment procedures on page 10 for detailed configuration steps:

1. Provision your FortiSASE instance and select the regions where your users will be located. Input licenses as needed.
2. Review the VPN overlay, BGP, and firewall policy configuration settings required by a FortiSASE SPA hub.
3. Convert the FortiGate NGFW to a FortiSASE SPA hub using the FortiOS Fabric Overlay Orchestrator feature.
4. Using the FortiSASE Private Access page, configure the FortiSASE security points of presence as spokes of the FortiGate SD-WAN Hub using its specific network attributes as parameters.
5. Configure the DNS settings to allow resolving hostnames for external and internal domains.
6. Verify IPsec VPN tunnels on the FortiGate SD-WAN hub(s).
7. Verify BGP routing on the FortiGate SD-WAN hub(s).
8. Test private access connectivity to the FortiGate SD-WAN network from remote users.

Deployment procedures

Provisioning your FortiSASE instance

Ensure that you have purchased the contract to provision FortiSASE, then do the following.

To provision your FortiSASE instance:

1. From the Fortinet Support site, register your FortiSASE contract.
2. Once registered, go to *Services* > *Cloud Services* > *FortiSASE* to provision your FortiSASE instance.
3. When provisioning, select the geographic location for your security sites and logging. Once provisioned, the FortiSASE dashboard displays your entitlement in the Remote User Management widget. The number of endpoints that the widget lists is the number of VPN users that are entitled to use this service.

Converting FortiGate NGFW to a FortiSASE SPA hub using FortiOS Fabric Overlay Orchestrator

This deployment guide only covers the FortiGate configuration for the BGP per overlay routing design.

This section describes how to use the Fabric Overlay Orchestrator feature in FortiOS 7.2.4 and later to convert the FortiGate NGFW to a FortiSASE SPA Hub. Since some VPN and BGP settings may not be configured by the Fabric Overlay Orchestrator, you will need to configure these settings later using the FortiOS CLI to complete the conversion.

For details on configuring using the FortiOS GUI without using the Fabric Overlay Orchestrator or FortiOS CLI, see Appendix C - Converting FortiGate NGFW configured using FortiOS GUI to a FortiSASE SPA hub without using the Fabric Overlay Orchestrator on page 65.

General steps

The following general steps should be used to configure a self-orchestrated SD-WAN overlay within a single Security Fabric.

These steps must be followed in this order and assume that the prerequisites and network topology above are in place.

1. Configure the root FortiGate using the Fabric Overlay Orchestrator.
2. Configure one or more downstream FortiGates using the Fabric Overlay Orchestrator.
3. Configure an overlay on spoke for additional incoming interface on hub (if applicable).
4. Verify the Fabric Overlay created by the Fabric Overlay Orchestrator:
   a. Verify IPsec VPN tunnels on the hub FortiGate.
   b. Verify BGP Routing on the hub FortiGate.
   c. Verify the Performance SLAs on the hub FortiGate.
   d. Verify IPsec VPN Tunnels on a spoke FortiGate.
   e. Verify BGP Routing on a spoke FortiGate.
   f. Verify the Performance SLA on a spoke FortiGate.

When configuring the root and downstream FortiGates, the Fabric Overlay Orchestrator configures the following settings in the background:

- IPsec overlay configuration (Hub-and-Spoke ADVPN tunnels)
- BGP configuration
- Policy routing
- SD-WAN zone
- SD-WAN performance SLAs

The FortiGate's role in the SD-WAN overlay is automatically determined by its role in the Security Fabric. The Fabric Root will have the role of the Hub and any first-level children (downstream devices) from the Fabric Root will have the role of a Spoke.

Policy creation

The Fabric Overlay Orchestrator can create firewall policies to allow all traffic through the SD-WAN overlay or create firewall policies just to allow health check traffic through it instead.

When enabling the Fabric Overlay Orchestrator on the root FortiGate device, you have three options for configuring the Policy creation setting: Automatic, Health Check (default), or Manual.

Policy creation option	Description
Automatic	Automatically creates policies for the loopback interface and tunnel overlays.
Health Check (default)	Automatically creates a policy for the loopback interface so SD-WAN health checks are functional.
Manual	No policies are created automatically.

The *Automatic* policy creation option creates wildcard allow policies for the tunnel overlays. Therefore, for some cases, these policies do not provide the granularity necessary to restrict overlay traffic to specific subnets or hosts.

When the Fabric Overlay Orchestrator has already been configured on a device, changing the policy creation rule will create new policies based on the rule but will not delete existing policies. Deleting existing policies must be performed manually.

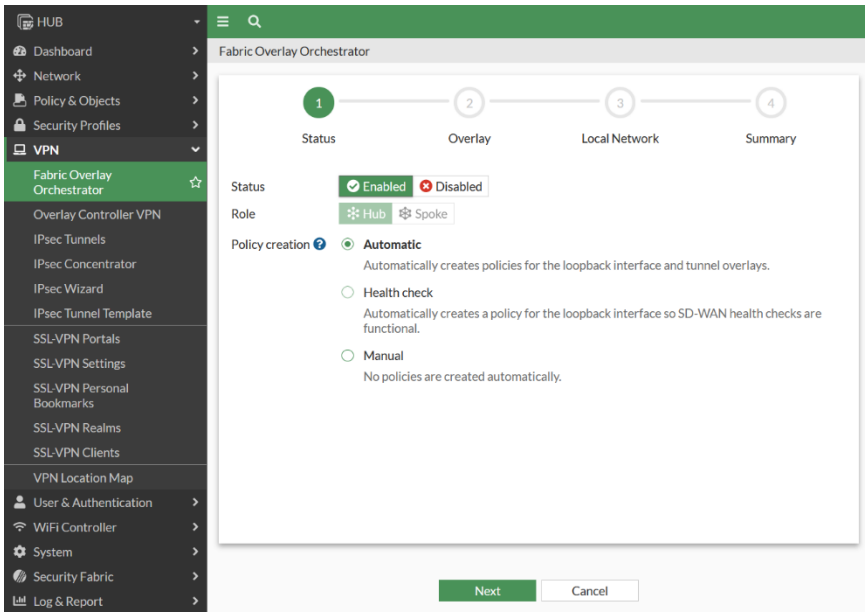
Configuring a root FortiGate using the Fabric Overlay Orchestrator

This deployment guide only covers the FortiGate configuration for the BGP per overlay routing design.

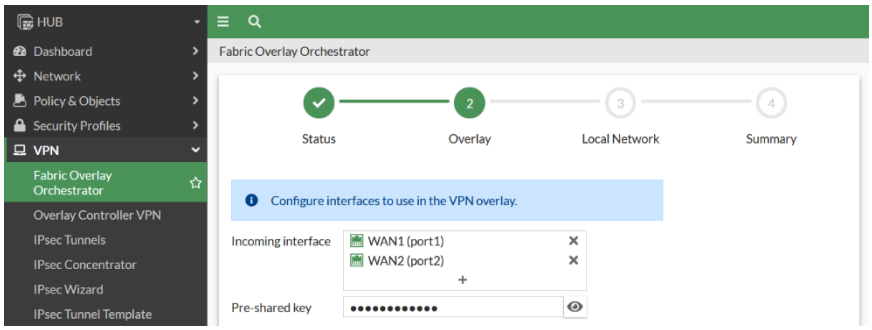
These steps describe how to run the Fabric Overlay Orchestrator on the root FortiGate.

To configure a root FortiGate using the Fabric Overlay Orchestrator:

1. Go to *VPN* > *Fabric Overlay Orchestrator*.
2. Set *Status* to *Enabled*. The *Role* is automatically selected depending on the FortiGate device's role in the Fortinet Security Fabric. When configuring the root FortiGate, confirm the *Role* is *Hub*. The Fabric root must always be the hub. For *Policy Creation*, select *Automatic*. Click *Next*.



3. For *Overlay*, select one or more interfaces as the *Incoming interface* or the underlay link over which the VPN overlay will be built, configure the *Pre-shared key*, and click *Next*. The example selects two incoming interfaces:

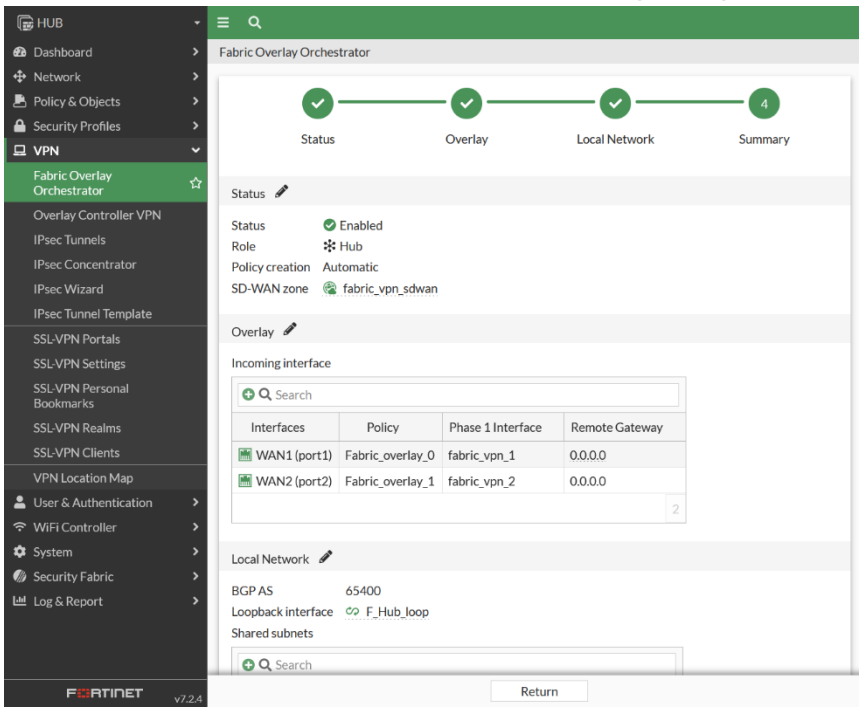


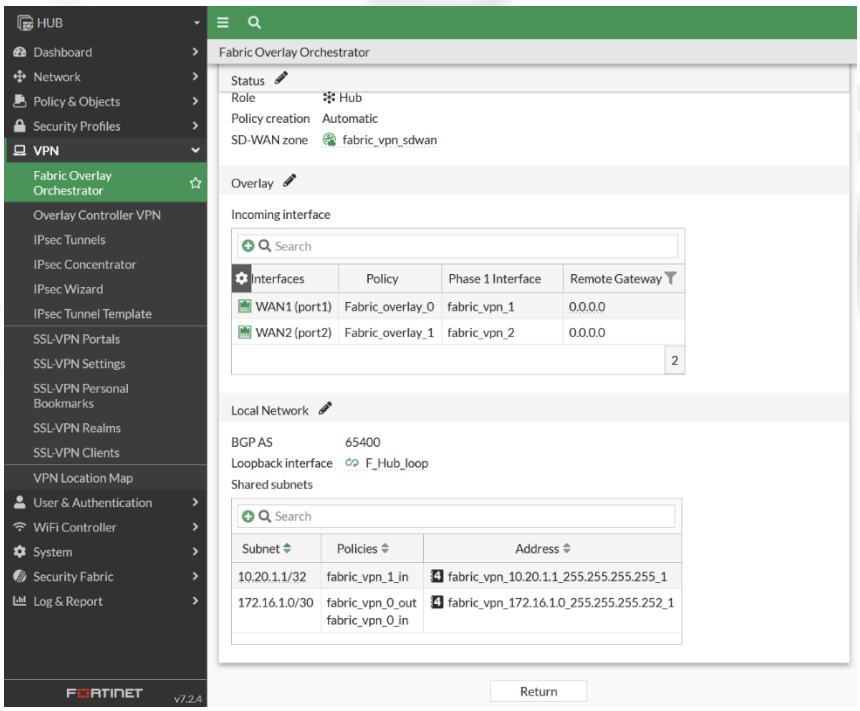
4. For *Local Network*, configure routing and local subnets to share with the VPN network, namely, the BGP AS, loopback address block, and shared interfaces settings:

Option	Description
BGP AS	Optionally, you can configure the BGP AS number. By default, this setting is set to 65400.
Loopback address block	Optionally, you can configure the loopback IP address. By default, this setting is set to 10.20.1.1/255.255.255.0.
Shared interfaces	Select the interface of the local network to share with the VPN network

Click *Next*.

5. For the first *Summary* step, review the configured settings and click *Apply*.
6. For the second *Summary* step, observe that the following settings have been created as follows:





Option	Description
SD-WAN Zone	*Status* > *SD-WAN* zone. In the example, this is fabric_vpn_sdwan.
VPN Tunnels	*Overlay* > *Incoming interface* > *Phase 1 Interface*. In the example, they are fabric_vpn1 and fabric_vpn2.
BGP	*Local Network* > *BGP AS*, *Local Network* > *Shared subnets*. In the example, the BGP AS is 65400 and subnets are 10.20.1.1/32 and 172.16.1.0/30.
Loopback Interface	*Local Network* > *Loopback interface*. In the example, it is F_Hub_loop.
Firewall Policies	*Overlay* > *Incoming interface* > *Policy*, *Local Network* > *Shared subnets* > *Policies*. In the example, they are Overlay: Fabric_overlay_0, Fabric_overlay_1, Shared subnets: fabric_vpn_1_in, fabric_vpn_0_out, fabric_vpn_0_in.

Configuring a downstream FortiGate using the Fabric Overlay Orchestrator

These steps describe how to run the Fabric Overlay Orchestrator on a downstream FortiGate.

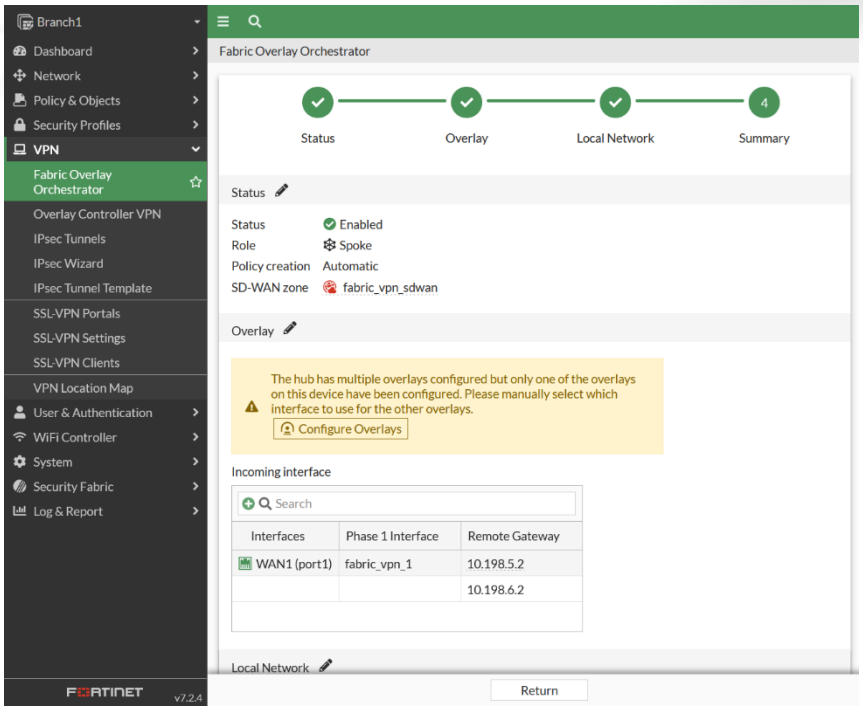
To configure a downstream FortiGate using the Fabric Overlay Orchestrator:

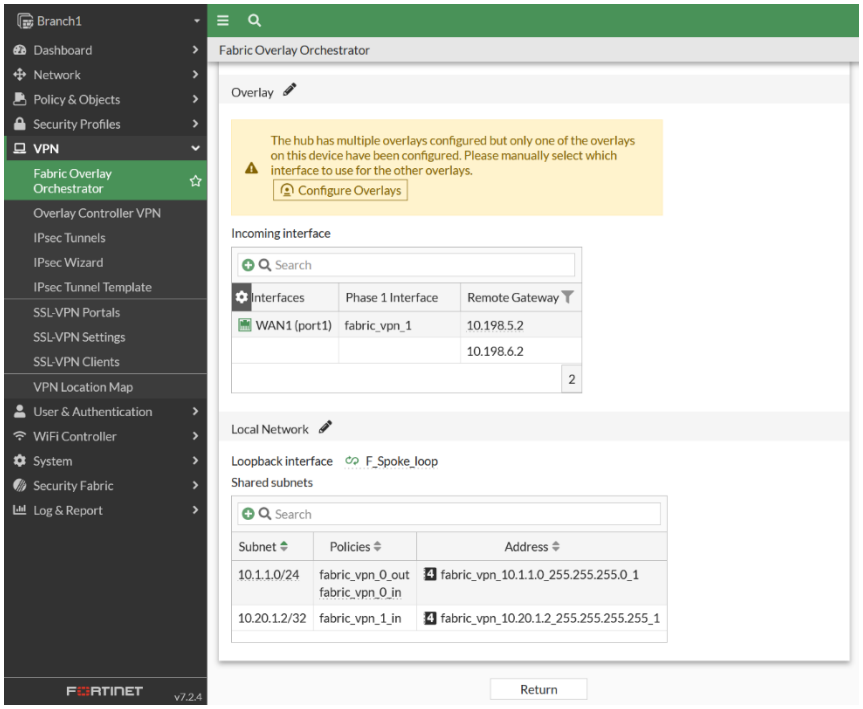
1. Go to *VPN* > *Fabric Overlay Orchestrator*.
2. Set *Status* to *Enabled*. The *Role* is automatically selected depending on the FortiGate device's role in the Fortinet Security Fabric. When configuring a downstream FortiGate, confirm the role is spoke. Only downstream FortiGates that are first-level children of the root may become spokes. Click *Next*.
3. For *Local Network*, configure routing and local subnets to share with the VPN network, namely, shared interfaces settings:

Option	Description
Shared interfaces	Select the interface of the local network to share with the VPN network

Click *Next*. Observe the *Configuring spoke Fabric VPN from root FortiGate notification* message.

4. For the first *Summary* step, review the configured settings and click *Apply*.
5. For the second *Summary* step, observe that the following settings have been created as follows:





Option	Description
SD-WAN Zone	*Status > SD-WAN* zone. In the example, this is fabric_vpn_sdwan.
VPN Tunnels	*Overlay > Incoming interface > Phase 1 Interface*. In the example, this is fabric_vpn1 .
BGP	*Local Network > BGP AS, Local Network > Shared subnets*. In the example, the BGP AS is 65400 and subnets are 10.1.10.0/24 and 10.20.1.2/32.
Loopback Interface	*Local Network > Loopback interface*. In the example, it is F_Spoke_loop.
Firewall Policies	*Local Network > Shared subnets > Policies*. In the example, they are fabric_vpn_1_in, fabric_vpn_0_out, fabric_vpn_0_in.

FortiOS generates the loopback IP addresses for the branches based on the index number of the trusted device in the hub Security Fabric system configuration. For example, if Branch1 is the first FortiGate and Branch2 is the second FortiGate authorized in the hub FortiGate, FortiOS generates the loopback addresses as follows:

FortiGate	Loopback IP address	Serial number
Branch1	10.20.1.2	FGVM02TM22009724
Branch2	10.20.1.3	FGVM02TM22009526

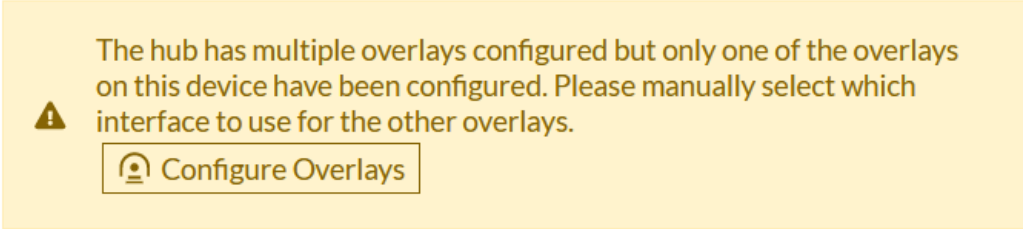
In this example, the Security Fabric trusted devices list in the Fabric-HUB FortiGate is as follows:

```
config system csf
    set status enable
    set group-name "fabric"
    config trusted-list
        edit "FGVM02TM22009724"
            set serial "FGVM02TM22009724"
            set index 1
        next
        edit "FGVM02TM22009526"
            set serial "FGVM02TM22009526"
            set index 2
        next
    end
end
```

Configuring an overlay on spoke for additional incoming interface on hub (if applicable)

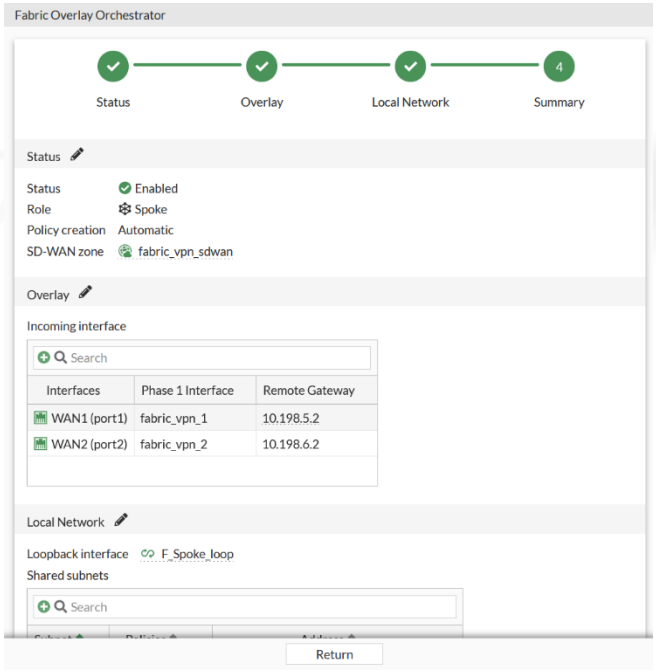
To configure an overlay on spoke for additional incoming interface on hub (if applicable):

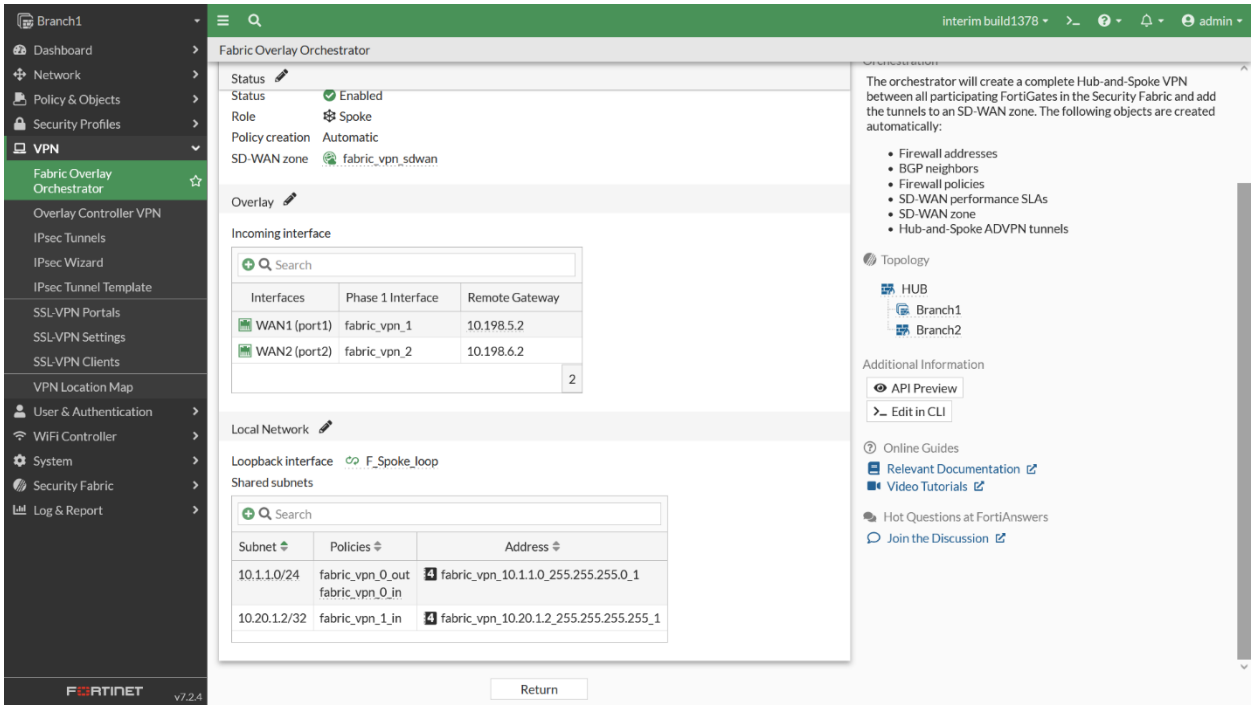
1. Typically, the hub will include two incoming interfaces. From the Fabric Overlay Orchestrator page, you will notice the following dialog:


The hub has multiple overlays configured but only one of the overlays on this device have been configured. Please manually select which interface to use for the other overlays.
Configure Overlays

You can configure an additional incoming interface (if applicable) using the GUI by clicking *Configure Overlays* in the dialog and adding the additional interface, such as WAN2 (port2), to the overlay.

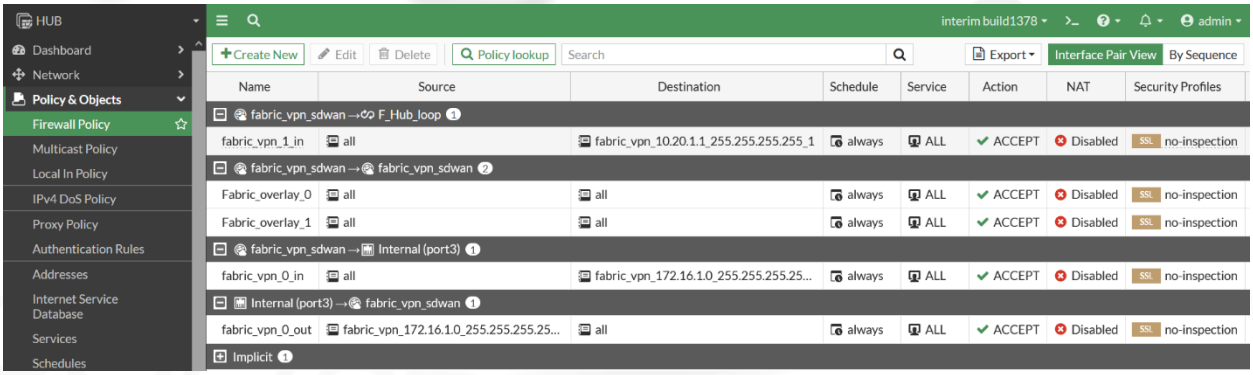
2. In the *Local Network* page, click *Next*.
3. In the *Summary* page, click *Apply*. You now see the following settings on the Summary page:





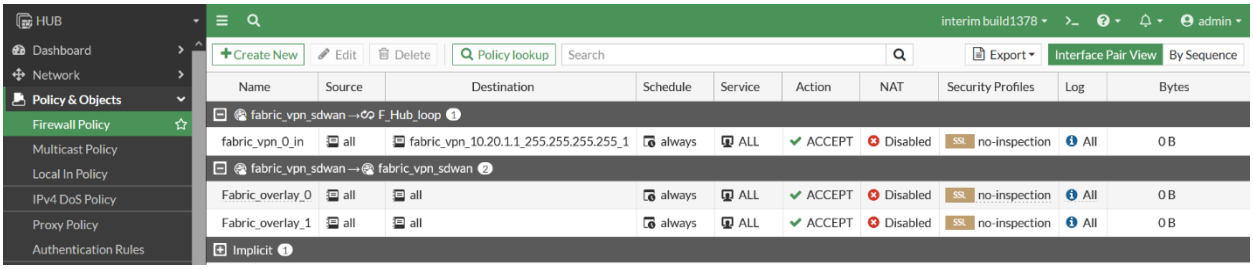
Verifying firewall policies on the hub FortiGate

On the hub, when *Policy creation* is set to *Automatic*, verify that wildcard firewall policies have been configured on the hub FortiGate. For this fabric overlay orchestrator configuration example using *Automatic*, the following firewall policies are configured on the hub FortiGate:



The *Automatic* policy creation option creates wildcard allow policies for the tunnel overlays. Therefore, for some cases, these policies do not provide the granularity necessary to restrict overlay traffic to specific subnets or hosts.

On the hub, when *Policy creation* is set to *Health Check*, verify that a single firewall policy allowing health check traffic to the hub's loopback has been configured on the hub FortiGate. For a fabric overlay orchestrator configuration example using *Health Check*, the following firewall policies are configured on the hub FortiGate:



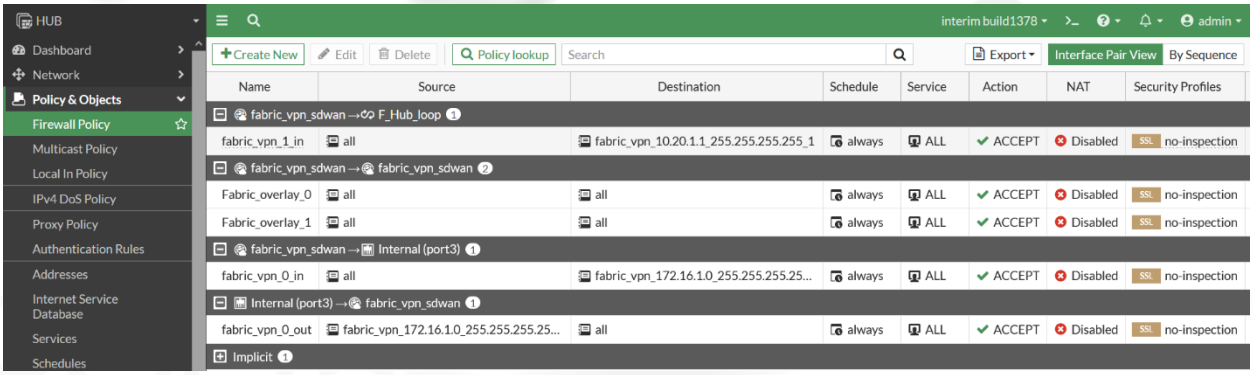
On the hub, when *Policy creation* is set to *Manual*, verify that no firewall policies were created by the fabric overlay orchestrator. Firewall policies must be manually configured on the hub FortiGate to allow traffic to the loopback interface for health checks and the overlays, if desired.

Verifying settings

After configuring the root and downstream FortiGates using the Fabric Overlay Orchestrator, you can verify settings on both hub and spoke.

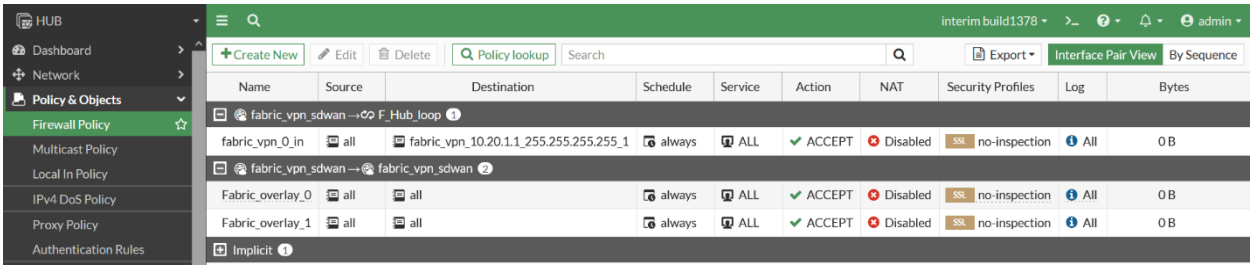
Verifying firewall policies on the hub FortiGate

On the hub, when *Policy creation* is set to *Automatic*, verify that wildcard firewall policies have been configured on the hub FortiGate. For this fabric overlay orchestrator configuration example using *Automatic*, the following firewall policies are configured on the hub FortiGate:



The *Automatic* policy creation option creates wildcard allow policies for the tunnel overlays. Therefore, for some cases, these policies do not provide the granularity necessary to restrict overlay traffic to specific subnets or hosts.

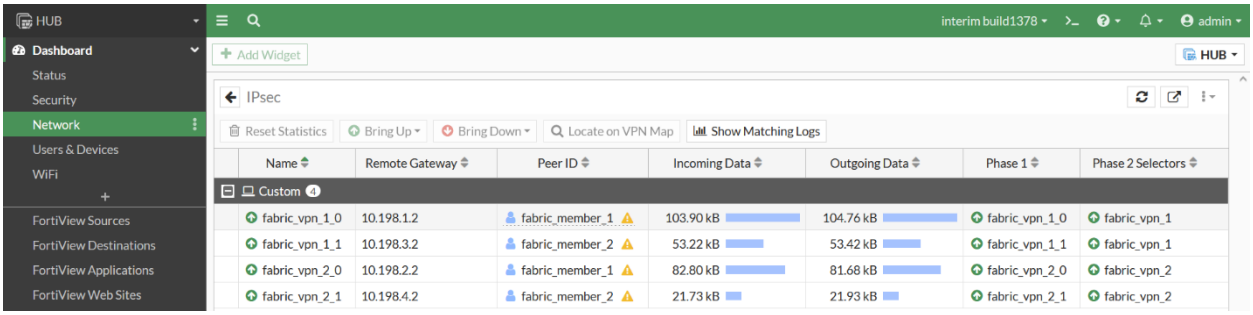
On the hub, when *Policy creation* is set to *Health Check*, verify that a single firewall policy allowing health check traffic to the hub's loopback has been configured on the hub FortiGate. For a fabric overlay orchestrator configuration example using *Health Check*, the following firewall policies are configured on the hub FortiGate:



On the hub, when *Policy creation* is set to *Manual*, verify that no firewall policies were created by the fabric overlay orchestrator. Firewall policies must be manually configured on the hub FortiGate to allow traffic to the loopback interface for health checks and the overlays, if desired.

Verifying IPsec VPN tunnels on the hub FortiGate

On a spoke, verify the IPsec tunnel back to the hub by going to *Dashboard* > *Network* and clicking on the IPsec widget to expand it:



There are two IPsec tunnels established with fabric_vpn_1_0 and fabric_vpn_1_1 and two IPsec tunnels established with fabric_vpn_2_0 and fabric_vpn_2_1 with <tunnel name>_0 and <tunnel name>_1 indicating the relative order in which these tunnels were established:

Tunnel name	Description
fabric_vpn_1_0	VPN tunnel listening on hub's WAN1 incoming interface, established with spoke 1 using its WAN1 interface
fabric_vpn_1_1	VPN tunnel listening on hub's WAN1 incoming interface, established with spoke 2 using its WAN1 interface
fabric_vpn_2_0	VPN tunnel listening on hub's WAN2 incoming interface, established with spoke 1 using its WAN2 interface
fabric_vpn_2_1	VPN tunnel listening on hub's WAN2 incoming interface, established with spoke 2 using its WAN2 interface

Verifying BGP routing on the hub FortiGate

To verify BGP routing on a hub FortiGate:

1. Check the BGP peering status and the advertised routes using the following CLI commands. Replace x.x.x.x with the BGP neighbor IP address:

   get router info bgp summary
   get router info bgp neighbors x.x.x.x advertised-routes

   The following provides sample output for these commands:

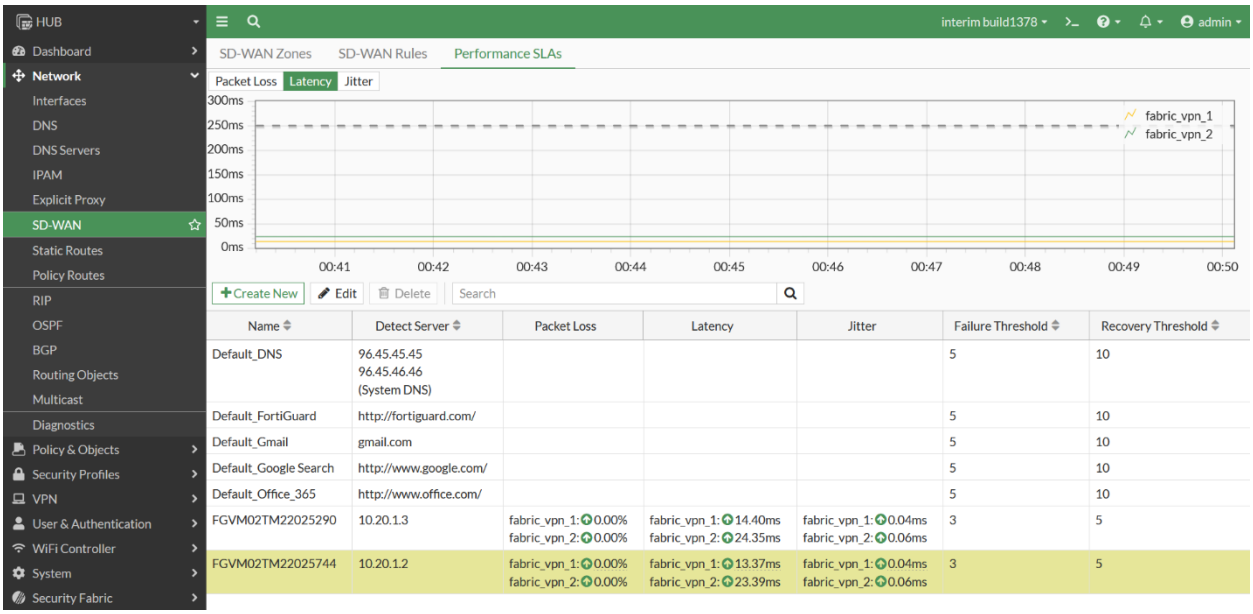
```
HUB # get router info bgp summary

VRF 0 BGP router identifier 10.20.1.1, local AS number 65400
BGP table version is 11
1 BGP AS-PATH entries
0 BGP community entries
Next peer check timer due in 43 seconds

Neighbor    V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.1 4      65400      23      27       11    0    0 00:09:28        2
10.10.10.2 4      65400      16      16       11    0    0 00:06:36        2
10.10.11.1 4      65400      14      20       11    0    0 00:09:22        2
10.10.11.2 4      65400       7      11       11    0    0 00:03:22        2

Total number of neighbors 4


HUB # get router info bgp neighbors 10.10.10.1 advertised-routes
VRF 0 BGP table version is 11, local router ID is 10.20.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*>i10.1.1.0/24      10.10.11.1                        100      0        0 i <-/2>
*>i10.1.2.0/24      10.10.11.2                        100      0        0 i <-/2>
*>i10.1.2.0/24      10.10.10.2                        100      0        0 i <-/1>
*>i10.10.10.0/24    10.10.10.253                      100  32768        0 i <-/1>
*>i10.10.11.0/24    10.10.10.253                      100  32768        0 i <-/1>
*>i10.20.1.1/32     10.10.10.253                      100  32768        0 i <-/1>
```

```
*>i10.20.1.2/32     10.10.11.1                100        0          0 i <-/2>
*>i10.20.1.3/32     10.10.11.2                100        0          0 i <-/2>
*>i10.20.1.3/32     10.10.10.2                100        0          0 i <-/1>
*>i172.16.1.0/30    10.10.10.253              100    32768          0 i <-/1>

Total number of prefixes 10
```

2. On the GUI, verify routing by going to *Dashboard* > *Networks*. Click the *Routing* widget to expand it, then select *BGP Neighbors* from the dropdown list in the top right corner.

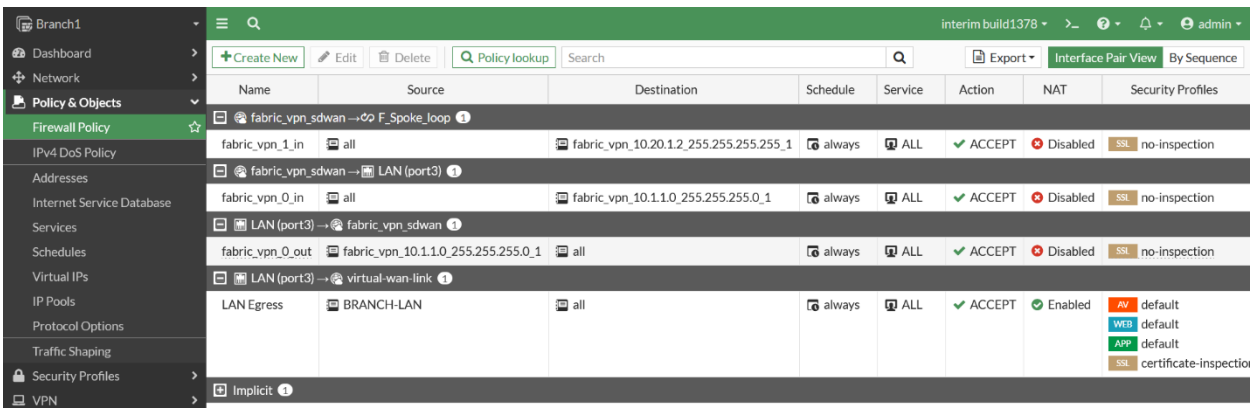
Verifying the performance SLAs on the hub FortiGate

On the hub, verify the performance SLAs are automatically created for each spoke named using the serial number of each spoke FortiGate by going to *Network* > *SD-WAN* and clicking the *Performance SLAs* tab:



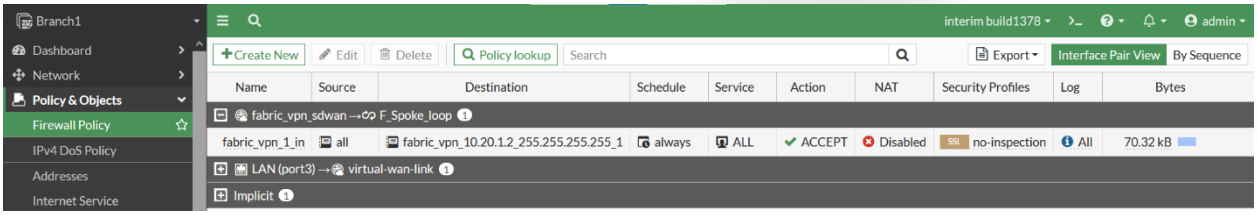
Verifying firewall policies on a spoke FortiGate

When *Policy creation* is set to *Automatic* on the hub FortiGate, verify that wildcard firewall policies have been configured on a spoke FortiGate. For this fabric overlay orchestrator configuration example using *Automatic*, the following firewall policies are configured on the spoke FortiGate:



The *Automatic* policy creation option creates wildcard allow policies for the tunnel overlays. Therefore, for some cases, these policies do not provide the granularity necessary to restrict overlay traffic to specific subnets or hosts.

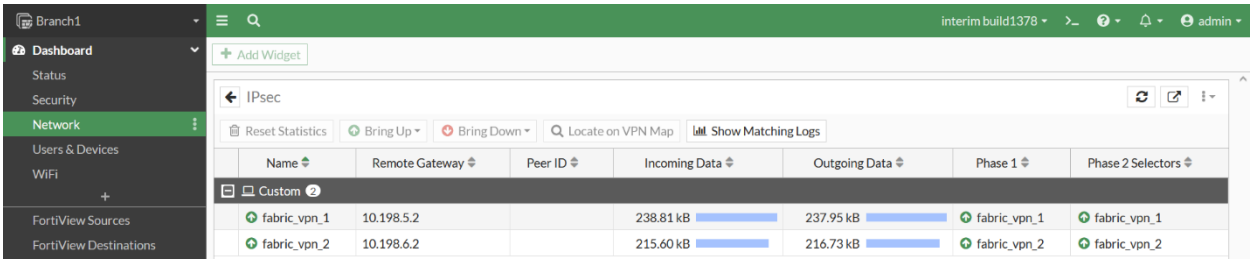
When *Policy creation* is set to *Health Check* on the hub FortiGate, verify that a single firewall policy allowing health check traffic to the spoke's loopback has been configured on a spoke FortiGate. For a fabric overlay orchestrator configuration example using *Health Check*, the following firewall policies are configured on the spoke FortiGate:



When *Policy creation* is set to *Manual* on the hub FortiGate, verify that no firewall policies were created by the fabric overlay orchestrator. Firewall policies must be manually configured on the spoke FortiGates to allow traffic to the loopback interface for health checks and the overlays, if desired.

Verifying IPsec VPN tunnels on a spoke FortiGate

On a spoke, verify the IPsec tunnel back to the hub by going to *Dashboard* > *Network* and clicking on the IPsec widget to expand it:



Verifying BGP routing on a spoke FortiGate

To verify BGP routing on a spoke FortiGate:

1. Check the BGP peering status and the advertised routes using the following CLI commands. Replace x.x.x.x with the BGP neighbor IP address:

   get router info bgp summary
   get router info bgp neighbors x.x.x.x advertised-routes

   The following provides sample output for these commands:

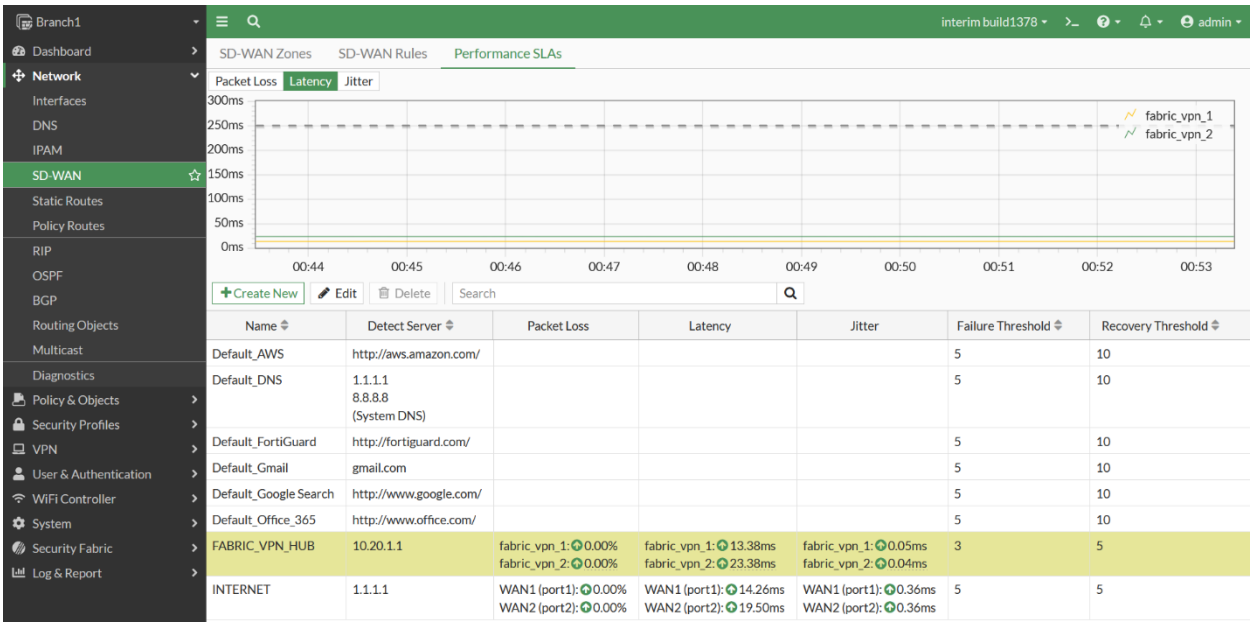
```
Branch1 # get router info bgp summary

VRF 0 BGP router identifier 10.20.1.2, local AS number 65400
BGP table version is 5
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.253 4      65400      41      37        4    0    0 00:23:39        8
```

```
10.10.11.253 4       65400       38       34         4     0     0 00:23:33         8

Total number of neighbors 2


Branch1 # get router info bgp neighbors 10.10.10.253 advertised-routes
VRF 0 BGP table version is 5, local router ID is 10.20.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*>i10.1.1.0/24      10.10.10.1                        100   32768         0 i <0/->
*>i10.20.1.2/32     10.10.10.1                        100   32768         0 i <0/->

Total number of prefixes 2
```

2. On the GUI, verify routing by going to *Dashboard* > *Networks*. Click the *Routing* widget to expand it, then select *BGP Neighbors* from the dropdown list in the top right corner.

Verifying the performance SLA on a spoke FortiGate

On the spoke, verify the performance SLA is automatically created for the hub FortiGate by going to *Network* > *SD-WAN* and clicking the *Performance SLAs* tab:



Verifying spoke-to-spoke ADVPN communication

To verify spoke-to-spoke ADVPN communication, run the following CLI commands on Spoke 1:

```
execute ping-options source <IP of interface on Spoke 1>
execute ping <IP of interface on Spoke 2>
get vpn ipsec tunnel summary
```

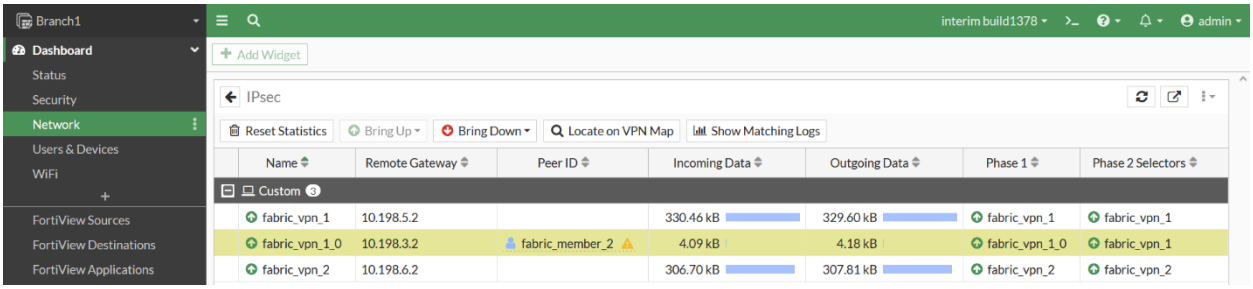
The following shows the expected output for this example:

```
Branch1 # exec ping-options source 10.20.1.2
```

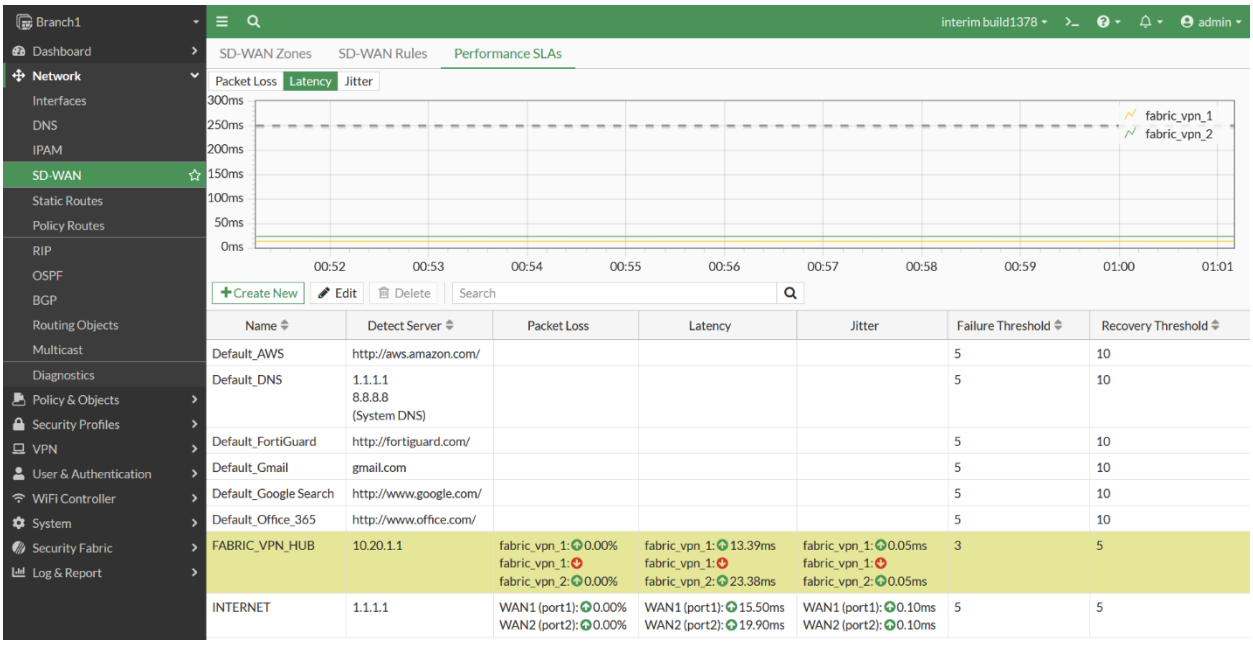
```
Branch1 # exec ping 10.20.1.3
PING 10.20.1.3 (10.20.1.3): 56 data bytes
64 bytes from 10.20.1.3: icmp_seq=0 ttl=254 time=27.7 ms
64 bytes from 10.20.1.3: icmp_seq=2 ttl=255 time=17.4 ms
64 bytes from 10.20.1.3: icmp_seq=3 ttl=255 time=17.5 ms
64 bytes from 10.20.1.3: icmp_seq=4 ttl=255 time=17.4 ms

--- 10.20.1.3 ping statistics ---
5 packets transmitted, 4 packets received, 20% packet loss
round-trip min/avg/max = 17.4/20.0/27.7 ms

Branch1 # get vpn ipsec tunnel summary
'fabric_vpn_1_0' 10.198.3.2:0  selectors(total,up): 1/1  rx(pkt,err): 25/0  tx(pkt,err):
26/2
'fabric_vpn_1' 10.198.5.2:0  selectors(total,up): 1/1  rx(pkt,err): 8032/0  tx(pkt,err):
8022/2
'fabric_vpn_2' 10.198.6.2:0  selectors(total,up): 1/1  rx(pkt,err): 7462/0  tx(pkt,err):
7478/1
```

fabric_vpn_1_0 is created for Spoke 1 to Spoke 2 communication.

On Spoke 1, verify the IPsec VPN tunnel between Spokes 1 and 2 by going to *Dashboard* > *Network* and clicking the IPsec widget to expand it:



On Spoke 1, verify the performance SLA has been updated by going to *Network* > *SD-WAN* and clicking the *Performance SLAs* tab:



The first fabric_vpn_1 corresponding to the spoke-to-hub VPN tunnel is shown as green and up. The second fabric_vpn_1 corresponding to the spoke-to-spoke VPN tunnel fabric_vpn_1_0 is shown as red and down since 10.20.1.1 is the IP address corresponding to the hub's loopback interface which is not present on another spoke.

Configuring SPA to the FortiGate SPA hub in FortiSASE Secure Private Access

Before configuring the *Secure Private Access* settings in the FortiSASE portal, to ensure proper secure private access (SPA) functionality, you must ensure that the FortiSASE SPA hub conforms to details mentioned in all previous sections of this guide up until this point, especially those sections covering Design concept and considerations on page 7, Product prerequisites on page 9, and Converting FortiGate NGFW to a FortiSASE SPA hub using FortiOS Fabric Overlay Orchestrator on page 10.

At this point, the FortiGate NGFW has been converted to a FortiSASE SPA Hub. Therefore, in the steps that follow, the FortiGate NGFW will now be referred to as the FortiSASE SPA Hub.

To allow FortiSASE remote users with secure private access (SPA) to resources behind your FortiGate SD-WAN hub network, you can configure FortiSASE security PoPs as spokes in your hub-and-spoke network using the *Secure Private Access* page.

Configuration workflow

To configure SPA service connections (hubs), you must follow this configuration workflow:

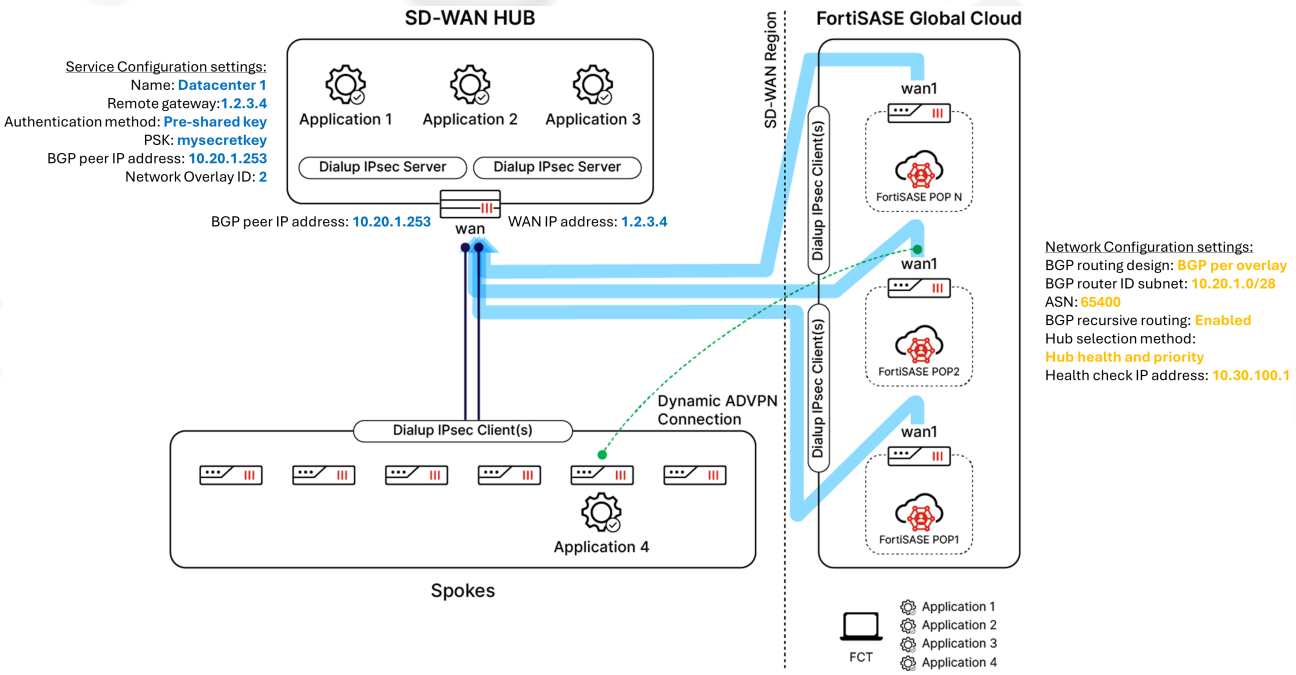
1. Under *Network* > *Network Configuration*, configure the common network configuration settings. See Configuring network configuration on page 26.
2. Under *Network* > *Secure Private Access*, click *Create*, and configure a new service connection (hub). See Configuring a new service connection on page 30.

You cannot configure a service connection or hub without first configuring *Network Configuration* settings.

BGP routing design

FortiSASE supports FortiGate hubs for SPA using *BGP per overlay* (default) or BGP on loopback. See the table for an overview of each routing design and example FortiGate hub and spoke reference configurations that you can use for a typical SD-WAN dual hub deployment:

BGP routing design overview	Example hub configuration for dual hub architecture	Example spoke configuration for dual hub architecture
BGP per overlay(default)	SD-WAN dual hub with VPN overlay and BGP routing - HUBs	SD-WAN dual hub with VPN overlay and BGP routing - Branches
BGP on loopback	BGP on loopback (Dual-Hub region) - Hub	BGP on loopback (Dual-Hub region) - Spoke



The example network topology uses the following settings configured in FortiSASE:

Configuration setting	Value used in example network topology
Network Configuration settings	
BGP routing design	*BGP per overlay*
BGP router ID subnet	10.20.1.0/28
Autonomous system number (ASN)	65400
BGP recursive routing	Enabled
Hub selection method	*Hub health and priority*
Health check IP address	10.30.100.1
Service Connection settings	
Name	Datacenter 1
Remote gateway	1.2.3.4
Authentication method	*Pre-shared key*
Pre-shared key	mysecretkey
BGP peer IP address	10.20.1.253
Network Overlay ID	2

Configuring network configuration

Before proceeding with configuring hubs or service connections, you must configure common secure private access (SPA) network configuration that all service connections use.

BGP routing design

FortiSASE supports FortiGate hubs for SPA using *BGP per overlay* (default) or BGP on loopback. See the table for an overview of each routing design and example FortiGate hub and spoke reference configurations that you can use for a typical SD-WAN dual hub deployment:

BGP routing design overview	Example hub configuration for dual hub architecture	Example spoke configuration for dual hub architecture
BGP per overlay(default)	SD-WAN dual hub with VPN overlay and BGP routing - HUBs	SD-WAN dual hub with VPN overlay and BGP routing - Branches
BGP on loopback	BGP on loopback (Dual-Hub region) - Hub	BGP on loopback (Dual-Hub region) - Spoke

You can use only one BGP routing design method for all hubs and spokes. You cannot mix them.

Also, you cannot change the BGP routing design method once you save it. You must delete the service connection(s) and network configuration and reconfigure with a different BGP routing design method.

To configure SPA network configuration:

Example values for SPA configuration settings are for illustrative purposes only. You must customize values to match those in your network environment.

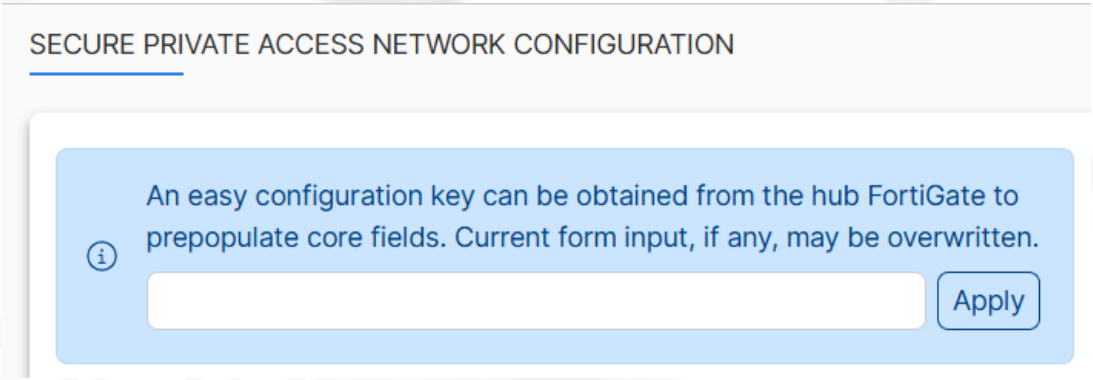
1. Go to *Network* > *Network Configuration*.
2. (Optional) You can use an easy configuration key to simplify SPA setup on FortiSASE by automatically populating key fields in *Network Configuration* and *Create Secure Private Access Service Connection* based on the FortiGate hub configuration. The easy configuration key is available on FortiOS 7.4.5 and later versions when the FortiGate is configured as a hub using Fabric overlay orchestrator. The FortiGate must have a valid SPA Service Connection license and be registered under the same FortiCloud account as FortiSASE. See SPA using a FortiSASE SPA hub with Fabric overlay orchestrator. You must set the following network attributes to use the key:
   a. Under *Network* > *Network Configuration*, set the following attributes. Otherwise, you cannot use the key:

Network attributes	Must be configured as...
BGP Routing Design	*BGP per overlay*
Hub Selection Method	*Hub Health and Priority*

   b. After configuring the attributes under *Network* > *Network Configuration*, you must configure the following authentication method under *Network* > *Secure Private Access* to use the easy configuration key:

Network attributes	Must be configured as...
Authentication Method	*Pre-shared Key*

   c. After completing the configuration on the hub FortiGate using Fabric overlay orchestrator, copy the key and paste it in *Network* > *Network Configuration* under the field in *Secure Private Access Network Configuration* on FortiSASE. See SPA easy configuration key for FortiSASE and SPA using a FortiSASE SPA hub with Fabric overlay orchestrator.


SECURE PRIVATE ACCESS NETWORK CONFIGURATION
An easy configuration key can be obtained from the hub FortiGate to prepopulate core fields. Current form input, if any, may be overwritten.
Apply

d. Click *Apply*. FortiSASE autopopulates fields such as *BGP Router ID Subnet*, *Autonomous System Number (ASN)*, and *Health Check IP* based off the FortiGate hub configuration. Click *Save* to finish SPA network configuration. You can proceed to Configuring a new service connection on page 30 without completing the remaining steps in this section.

3. Under *Network* > *Network Configuration*, under the *Secure Private Access Network Configuration* page, for *BGP Routing Design*, select one of the following:
   - BGP per overlay (default selection)
   - BGP on loopback. FortiSASE automatically selects and grays out *BGP Recursive Routing* after you selecting this option.
4. Fill in the rest of the fields with values of the attributes of the FortiGate hub network connection. FortiSASE performs input validation and notifies you of any invalid values. See the following table:

Network attributes	Description	Example
BGP Routing Design	FortiSASE supports these main routing design methods: • BGP per overlay (default) • BGP on loopback You can use only a single BGP routing design method for all hubs and spokes. You cannot mix them. See Routing design methods.	BGP per overlay
BGP router ID subnet	For *BGP per overlay*, available/unused subnet that can be used to assign loopback interface IP addresses used for BGP router IDs parameter only on the FortiSASE security PoPs. /28 is the minimum subnet size. Typically, this BGP router ID subnet is a subnet within the overall BGP loopback summary range that is currently unused. For example, if the BGP loopback summary range is 10.20.1.0/24 then you can choose to configure 10.20.1.0/28 as the BGP router ID subnet if it is unused. For *BGP on loopback*, you must configure this subnet as a neighbor range in the hub BGP settings.	10.20.1.0/28
Autonomous system number (ASN)	BGP autonomous system (AS) number of your hubs. Typically, this should be the same on both hubs.	65400

Network attributes	Description	Example
BGP recursive routing	Enabling the BGP recursive routing setting allows for interhub connectivity and redundancy to networks behind the active hub if each hub has a physical connection to the others for cases when connectivity between a FortiSASE security PoP and the active hub fails. For example, consider that this BGP configuration setting enabled and a FortiSASE security PoP's connectivity with hub 1 goes down. To ensure the security PoP can reach a network behind hub 1, it would route traffic to hub 2 first, then route it to hub 1 via its interhub connection, followed by routing the traffic to the desired destination network behind hub 1.	Enabled
Hub selection method	Method by which FortiSASE selects hub. By default, FortiSASE uses hub health and priority: • **Hub health and priority**: periodically obtain jitter, latency, and packet loss measurements for each hub via the health check IP address. FortiSASE selects the highest priority hub within each PoP that meets lowest cost (SLA). A hub can be assigned a different priority level in different PoPs. • **BGP MED**: BGP multi-exit discriminator (MED) is an attribute that an autonomous system advertising routes to another peer sets. FortiSASE learns MED from the configured hubs. See BGP multi-exit discriminator.	Hub health and priority
Health check IP address	IP address of a server behind the hub that should be used to set up the SD-WAN performance SLA rule. On the hub, you can configure a loopback interface for health check purposes and specify the IP address of that loopback interface for this parameter. Since there is only a single health check IP address, you can configure a loopback on all hubs with the same IP address. Also, in the hub configuration, you will need to create a policy to allow traffic from the IPsec tunnel to this loopback interface.	10.30.100.1

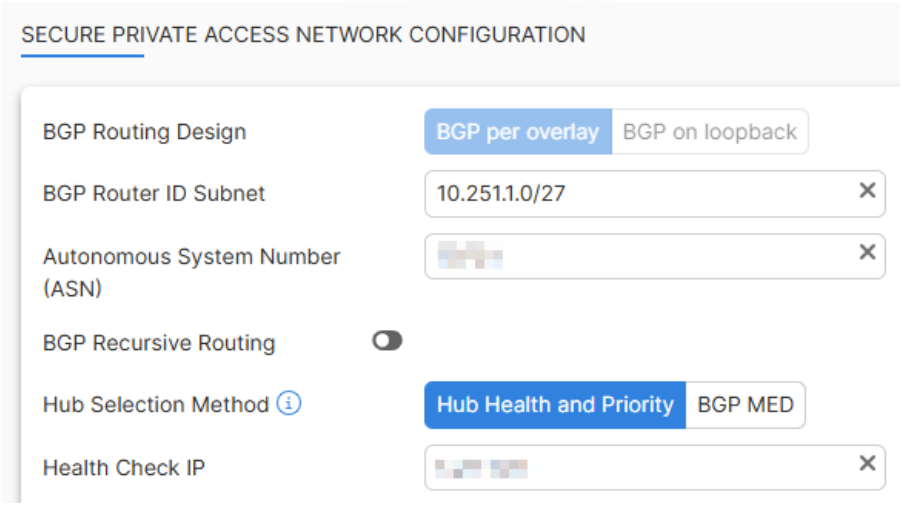
As some IP addresses ranges are reserved for FortiSASE internal usage, note the network restrictions in Network restrictions.

For *BGP per overlay*, the BGP router ID subnet should not overlap with the subnet used for the BGP peer IP address. These settings should be unique values as the example values demonstrate.

For *BGP on loopback*, the BGP router ID subnet should match the BGP peer IP address range defined on the hub.

When using the BGP MED option, user-defined hub priorities are not used because the SD-WAN SLA rule is disabled in this case.

5. Click *Save*.



Configuring a new service connection

You can create a new service connection (hub) using one of the following BGP routing design methods:

- BGP per overlay (default)
- BGP on loopback

You configured the corresponding BGP routing design method in *Network > Network Configuration*.

After you create a service connection, you can update its authentication method using *Update Authentication Method*, namely, to switch from using a preshared key (PSK) to a certificate or vice-versa. You can also use this option to update the existing authentication method's settings, such as updating the PSK or updating the PKI user or certificate.

To configure service connections or hubs for BGP per overlay:

Example values for SPA configuration settings are for illustrative purposes only. You must customize values to match those in your network environment.

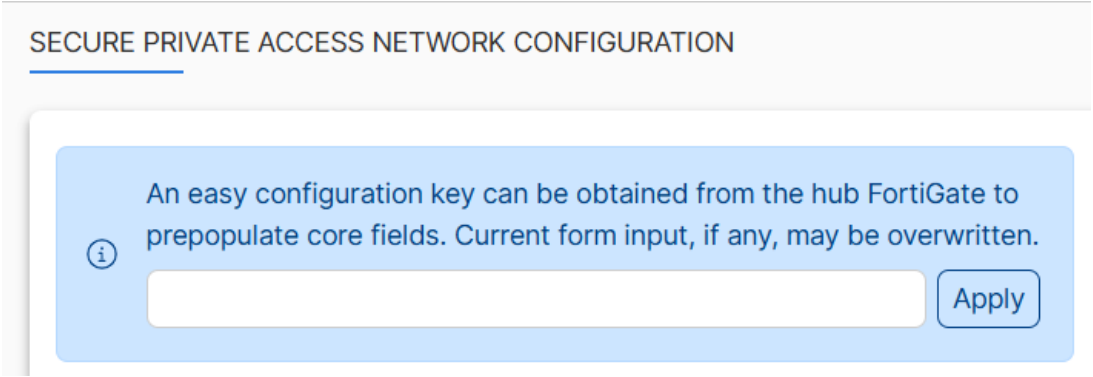
1. Go to *Network* > *Secure Private Access*.
2. Click *Create*.
3. (Optional) You can use an easy configuration key to simplify SPA setup on FortiSASE by automatically populating key fields in *Network Configuration* and *Create Secure Private Access Service Connection* based on the FortiGate hub configuration. The easy configuration key is available on FortiOS 7.4.5 and later versions when the FortiGate is configured as a hub using Fabric overlay orchestrator. The FortiGate must have a valid SPA Service Connection license and be registered under the same FortiCloud account as FortiSASE. See SPA using a FortiSASE SPA hub with Fabric overlay orchestrator. You must set the following network attributes to use the key:
   a. Under *Network* > *Network Configuration*, set the following attributes. Otherwise, you cannot use the key:

Network attributes	Must be configured as...
BGP Routing Design	*BGP per overlay*
Hub Selection Method	*Hub Health and Priority*

   b. After configuring the attributes under *Network* > *Network Configuration*, you must configure the following authentication method under *Network* > *Secure Private Access* to use the easy configuration key:

Network attributes	Must be configured as...
Authentication Method	*Pre-shared Key*

   c. After completing the configuration on the hub FortiGate using Fabric overlay orchestrator, copy the key and paste it in *Network* > *Network Configuration* under the field in *Secure Private Access Network Configuration* on FortiSASE. See SPA easy configuration key for FortiSASE and SPA using a FortiSASE SPA hub with Fabric overlay orchestrator.


SECURE PRIVATE ACCESS NETWORK CONFIGURATION
An easy configuration key can be obtained from the hub FortiGate to prepopulate core fields. Current form input, if any, may be overwritten.
Apply

   d. Click *Apply*. FortiSASE autopopulates fields such as *BGP Router ID Subnet*, *Autonomous System Number (ASN)*, and *Health Check IP* based off the FortiGate hub configuration. Click *Save* to finish SPA network configuration. You can proceed to Configuring a new service connection on page 30 without completing the remaining steps in this section.
4. Fill in the rest of the fields with the attributes of the FortiGate hub or service connection. FortiSASE validates the input and notifies you of any invalid values.

Network attributes	Description	Example
Name	Alias or comment associated with the hub. Maximum length of 25 characters with acceptable characters being alphanumeric characters, spaces, and dashes (-).	Datacenter 1

Network attributes	Description	Example
Remote gateway	IPsec VPN remote gateway (public IP address) for the hub.	1.2.3.4
Authentication method	Method used to authenticate with the FortiGate hub. Supports *Pre-shared key* (default) and *Certificate*.	Pre-shared key
Pre-shared key (PSK)	When *Authentication Method* is configured as *Pre-shared key*, define the hub PSK.	mysecretkey
PKI User	When *Authentication Method* is configured as *Certificate*, select the PKI user with valid subject and CA certificate used by FortiSASE to validate the hub's certificate. You can directly create the PKI user from *+Create* or via *Configuration > PKI*, then select it here.	mypeer
Certificate	When *Authentication Method* is configured as *Certificate*, select the certificate to be presented by the FortiSASE security PoP. You must import this certificate into FortiSASE via *System > Certificates* as a *Local Certificate*.	Fortinet_Factory
ADVPN Route Tag	For *BGP on loopback* only, ADVPN route tag number for spoke to tag incoming routes advertised from a hub. See Enhanced BGP next hop updates and ADVPN shortcut override.	1
BGP peer IP address	On the hub, the IP address used as the BGP peer ID	10.20.1.253
Network overlay ID	Define a unique network ID for each hub. If a active hub triggers a shortcut between two spokes and there is a failover to another hub which also triggers a shortcut between the same two spokes, the latter shortcut connection fails if both hubs have the same network ID. Ensure that the IPsec VPN tunnels towards each hub have different network overlay IDs.	2

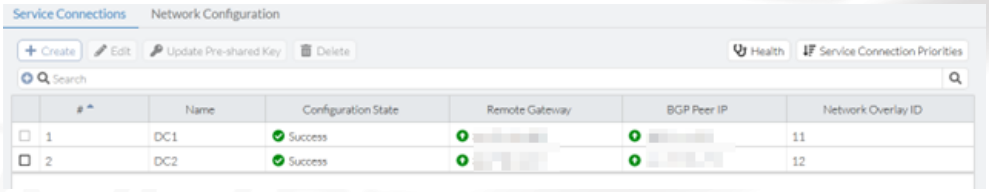
As some IP addresses ranges are reserved for FortiSASE internal usage, note the network restrictions in Network restrictions.

For *BGP per overlay*, the BGP router ID subnet should not overlap with the subnet used for the BGP peer IP address. These settings should be unique values as the example values demonstrate.

For *BGP on loopback*, the BGP router ID subnet should match the BGP peer IP address range defined on the hub.

5. Click *Save*.

6. Once FortiSASE successfully configures the service connection, it notifies you. The value in the *Configuration State* column changes from *Creating* to *Success*.
7. (Optional) Repeat the steps to configure up to a total of twelve service connections as necessary to support your secure private access service connection network topology. The following shows the GUI after configuring two service connections:



For FortiSASE security points of presence (PoP), the SD-WAN performance SLA (health check) setting has the following ㅇㄷㄹ며 | ㅅ parameters:

- **Latency threshold**: 120 ms
- **Jitter threshold**: 55 ms
- **Packet loss threshold**: 1%

You can edit these parameters in FortiSASE. See Editing SLA thresholds on page 36.

Also, for FortiSASE security PoPs, the SD-WAN rule is configured with the lowest cost (SLA) mode, where the security PoPs choose the lowest cost link (highest priority hub) that satisfies the SLA to forward traffic.

In the SD-WAN rule used by each FortiSASE security PoP, the interface preference order matters when selecting links of equal cost (equal priority hubs). Therefore, to define interface preference order, you must configure service connections in FortiSASE in the desired order of preference from the most preferred hub to the least preferred hub.

To configure service connections or hubs for BGP on loopback:

Example values for SPA configuration settings are for illustrative purposes only. You must customize values to match those in your network environment.

1. Go to *Network* > *Secure Private Access*.
2. Click *Create*.
3. For the *Create Secure Private Access Service Connection* step, fill in the fields with the attributes of the FortiGate hub or service connection. FortiSASE performs input validation and notifies you of any invalid values.

Network attributes	Description	Example
Name	Alias or comment associated with the hub. Maximum length of 25 characters with acceptable characters being alphanumeric characters, spaces, and dashes (-).	Datacenter 1
Remote gateway	IPsec VPN remote gateway (public IP address) for the hub.	1.2.3.4
Authentication method	Method used to authenticate with the FortiGate hub. Supports *Pre-shared key* (default) and *Certificate*.	Pre-shared key

Network attributes	Description	Example
Pre-shared key (PSK)	When *Authentication Method* is configured as *Pre-shared key*, define the hub PSK.	mysecretkey
PKI User	When *Authentication Method* is configured as *Certificate*, select the PKI user with valid subject and CA certificate used by FortiSASE to validate the hub's certificate. You can directly create the PKI user from *+Create* or via *Configuration > PKI*, then select it here.	mypeer
Certificate	When *Authentication Method* is configured as *Certificate*, select the certificate to be presented by the FortiSASE security PoP. You must import this certificate into FortiSASE via *System > Certificates* as a *Local Certificate*.	Fortinet_Factory
ADVPN Route Tag	For *BGP on loopback* only, ADVPN route tag number for spoke to tag incoming routes advertised from a hub. See Enhanced BGP next hop updates and ADVPN shortcut override.	1
BGP peer IP address	On the hub, the IP address used as the BGP peer ID	10.20.1.253
Network overlay ID	Define a unique network ID for each hub. If a active hub triggers a shortcut between two spokes and there is a failover to another hub which also triggers a shortcut between the same two spokes, the latter shortcut connection fails if both hubs have the same network ID. Ensure that the IPsec VPN tunnels towards each hub have different network overlay IDs.	2

As some IP addresses ranges are reserved for FortiSASE internal usage, note the network restrictions in Network restrictions.

For *BGP per overlay*, the BGP router ID subnet should not overlap with the subnet used for the BGP peer IP address. These settings should be unique values as the example values demonstrate.

For *BGP on loopback*, the BGP router ID subnet should match the BGP peer IP address range defined on the hub.

4. Click *Save*.
5. Once FortiSASE successfully configures the service connection, it notifies you. The value in the *Configuration State* column changes from *Creating* to *Success*.
6. (Optional) Repeat the steps to configure up to a total of twelve service connections as necessary to support your secure private access service connection network topology.

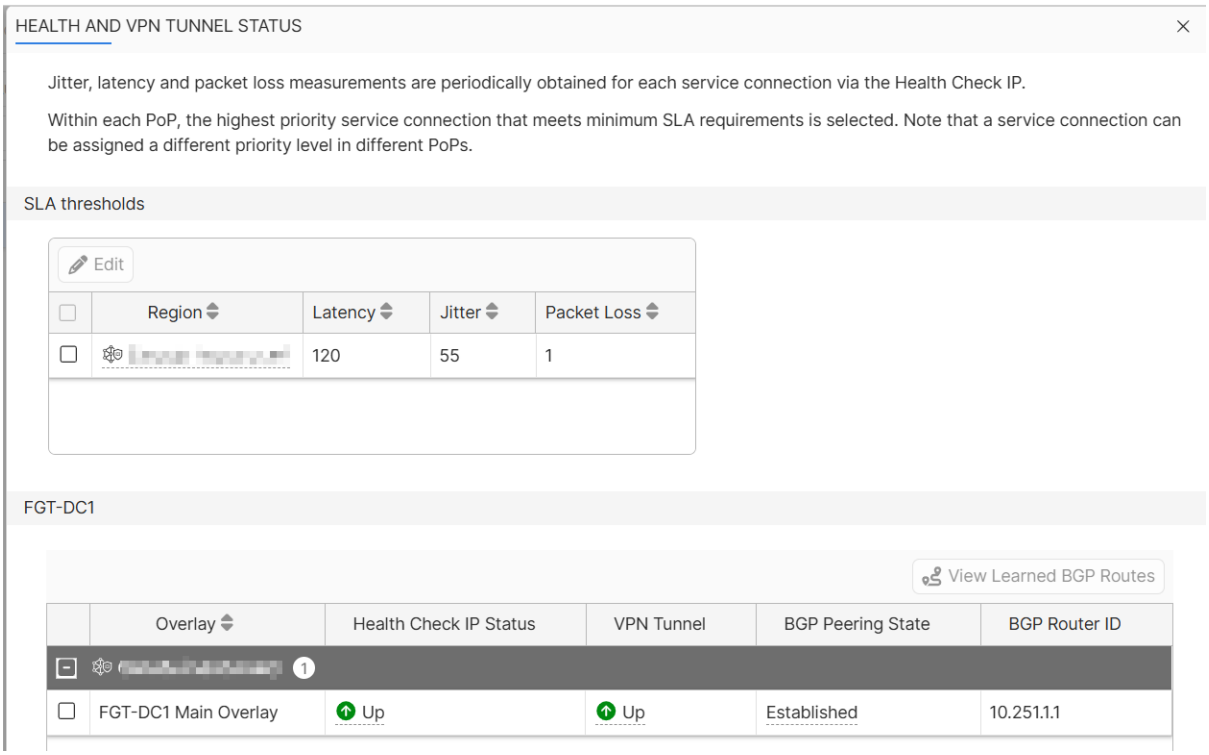
To update the authentication method settings for a service connection:

1. Go to *Network* > *Secure Private Access*.
2. Click *Update Authentication Method*.
3. Select the *Authentication Method* and configure the corresponding parameter(s):
   a. *New Pre-shared Key* when *Pre-shared Key* is selected.
   b. *PKI User* and *Certificate* when *Certificate* is selected.
4. Click *OK*. Once FortiSASE successfully updates the authentication method for the service connection, it notifies you with the message *Authentication method updated successfully*.

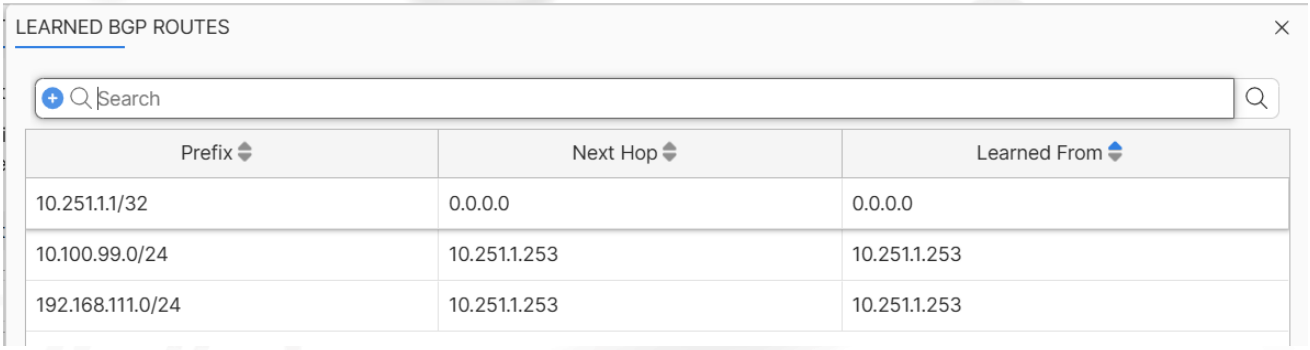
Viewing health and VPN tunnel status

Click the *Health* button at the top of the page to view the *Health and VPN Tunnel Status* page, which shows all configured hubs' health and VPN tunnel status. This page provides advanced monitoring of the IPsec VPN tunnel, BGP peering state, and health check IP status that you can use for troubleshooting advanced scenarios with configured hubs.

For example, you can view two hubs' health and VPN tunnel status from this page:



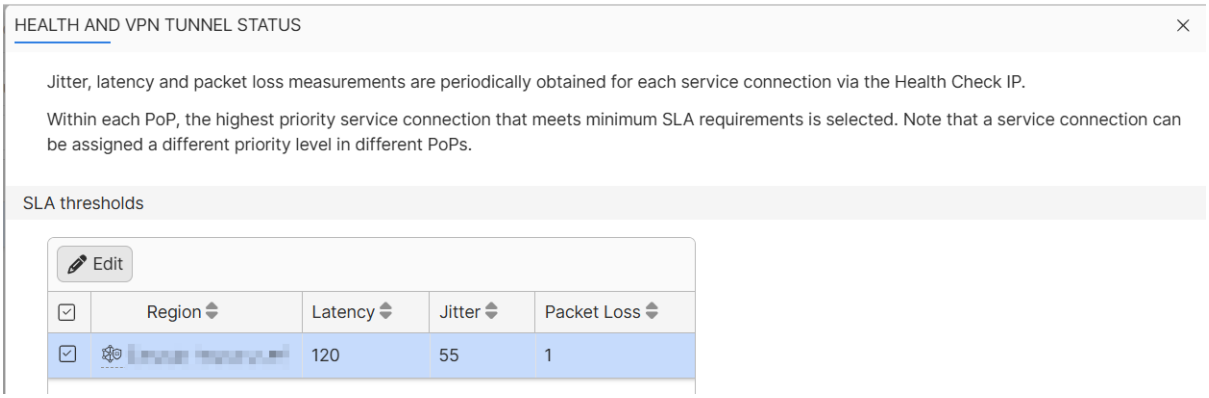
For any hub, selecting a point of presence and clicking *View Learned BGP Routes* displays the learned BGP routes for that hub. For example, the learned BGP routes for the example DC1 are as follows:



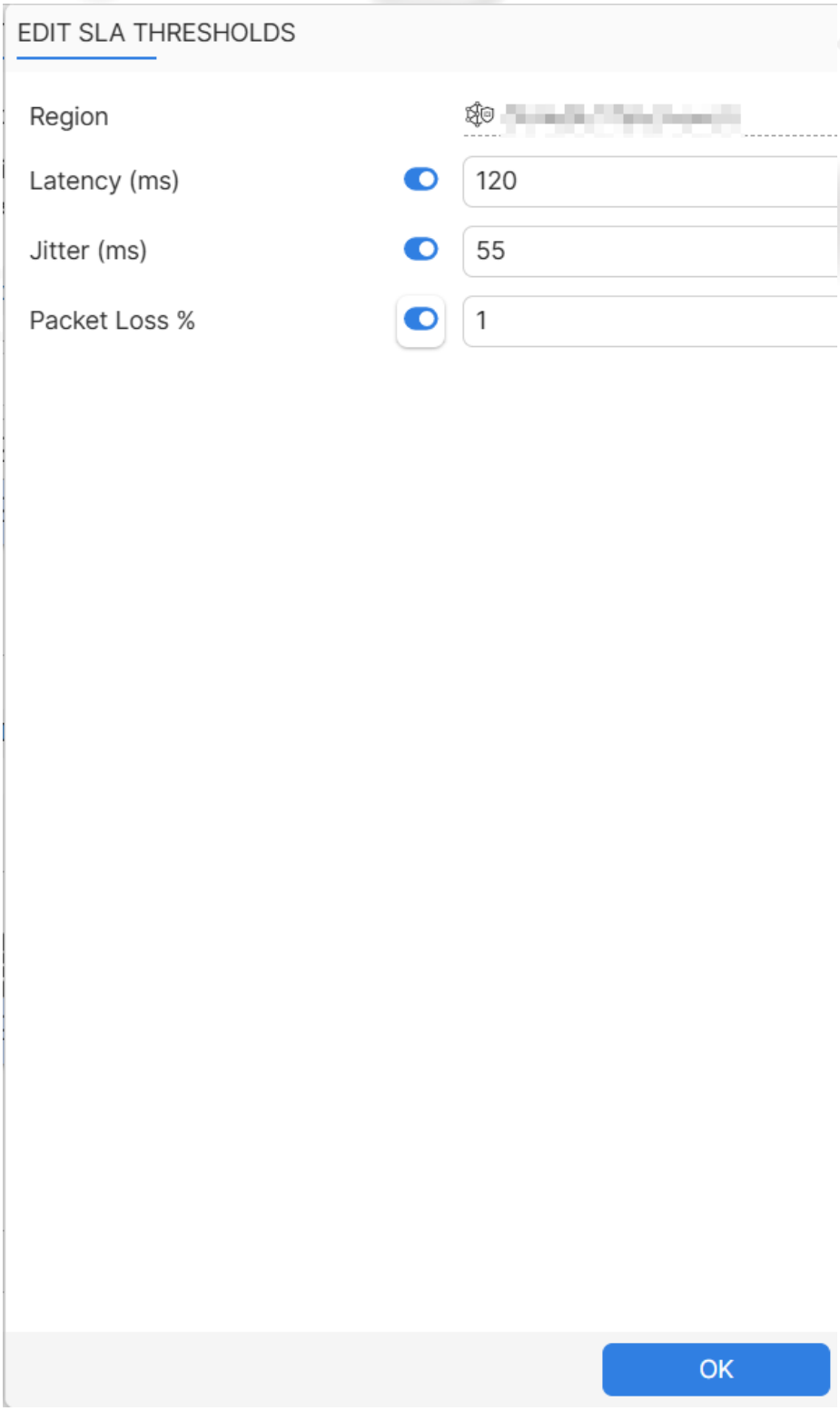
Editing SLA thresholds

You can customize latency, jitter, and packet loss SLA thresholds per security point of presence (PoP) used for secure private access hub SD-WAN health checks when *Hub Selection Method* is *Hub Health and Priority*. See Configuring network configuration on page 26.

SLA thresholds can be edited from *Network* > *Secure Private Access* by selecting a service connection and clicking *Health*, and then selecting a security PoP and clicking *Edit* to edit the SLA thresholds.


HEALTH AND VPN TUNNEL STATUS
Jitter, latency and packet loss measurements are periodically obtained for each service connection via the Health Check IP.
Within each PoP, the highest priority service connection that meets minimum SLA requirements is selected. Note that a service connection can be assigned a different priority level in different PoPs.
SLA thresholds
Edit
Region
Latency
Jitter
Packet Loss
120
55
1

In the *Edit SLA Thresholds* slide-in, the default SLA threshold values are listed. You can edit each threshold by enabling it, entering a suitable value and clicking *OK*.

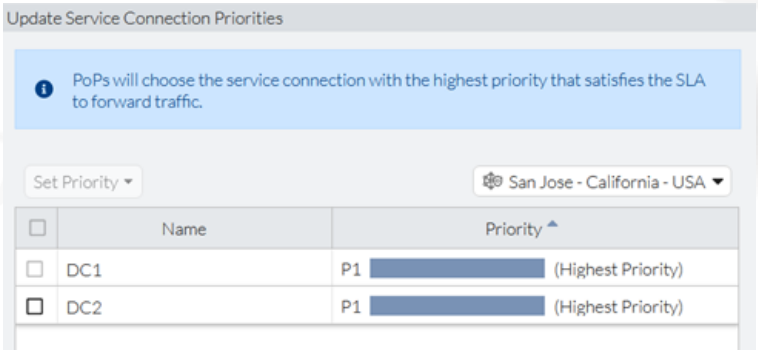


Updating service connection priorities

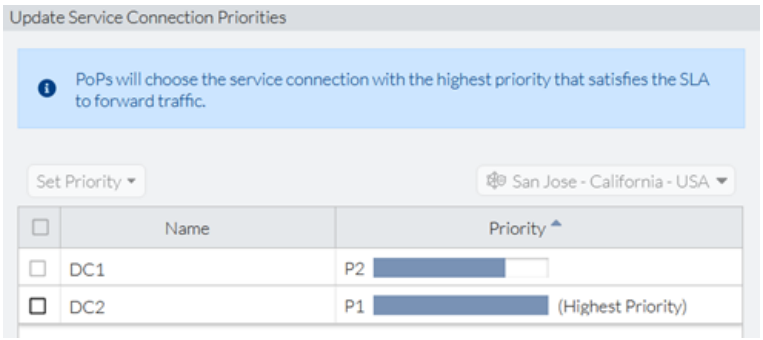
When you configure the hub selection method as hub health and priority within each point of presence (PoP), FortiSASE selects the highest priority hub that meets minimum SLA requirements. You can assign a hub a different priority level in different PoPs using the *Service Connection Priorities* page. A lower numerical cost value indicates a higher priority for a hub and vice-versa.

To update hub priorities:

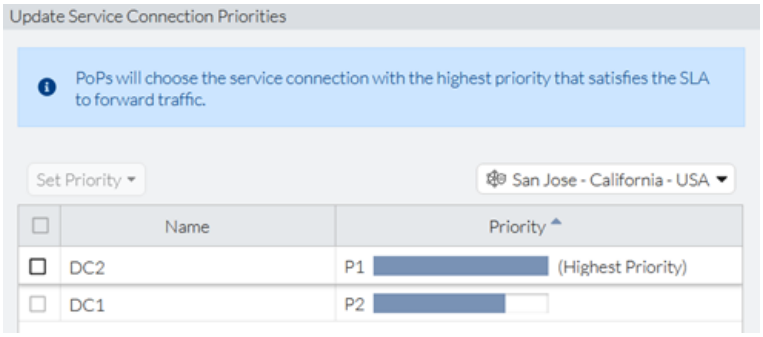
1. Go to *Network* > *Secure Private Access*. Click *Service Connection Priorities*.
2. From the *Security PoP* dropdown list, select the desired PoP hub. The example selects the San Jose – California – USA security PoP.



3. Select the desired hub and do one of the following to set the priority. P1 is the highest priority, and P2 is the lowest priority
   a. From the *Set Priority* dropdown list, select the desired priority.
   b. Right-click the hub, select *Set Priority*, and select the desired priority.
4. Set the priority for each hub that will influence hub selection. The example modifies the hub priorities so that the priority of DC1 is P2 and the priority of DC2 is P1:



5. Click *Apply* to save the updated priority values. The page sorts the hubs from highest to lowest priority:



6. (Optional) Repeat the steps to update hub priorities for other security PoPs.

Deleting a hub configuration

You cannot directly update hub configuration. You must delete any current configuration and reconfigure using new settings to update it.

To delete a hub configuration:

1. Go to *Network* > *Secure Private Access*.
2. Select the desired hub(s).
3. Click *Delete*.
4. In the confirmation dialog, click *OK*. The *Configuration State* column value for the hub changes from *Up* to *Deleting*. After a moment, FortiSASE removes the hub's table entry and deletes the hub configuration.

Configuring SPA using the REST API

A FortiSASE administrator can perform secure private access (SPA) configuration using the FortiSASE REST API to manage the common SPA network connection and SPA service connections to FortiGate SPA hubs and to retrieve the status of these connections. See Appendix B - REST API.

All SPA configuration operations are possible in the REST API except for viewing health and VPN tunnel status.

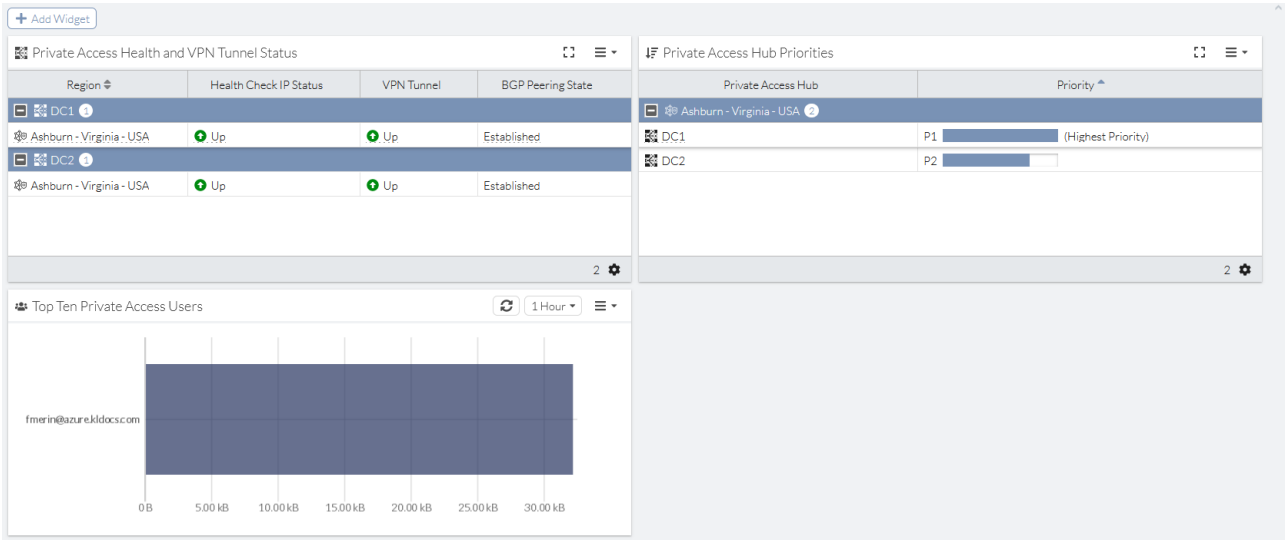
Only BGP on loopback supports multiple IPsec overlays in the REST API.

Monitoring private access hubs

To monitor private access hubs when they have been configured, view the following widgets in *Dashboards* > *Private Access*:

- Private Access Health and VPN Tunnel Status
- Private Access Hub Priorities
- Top Ten Private Access Users

For example, the following provides private access widgets with data for two private access hubs:



Configuring a private access policy for client-to-server traffic

Secure private access (SPA) client-to-server communication is the typical SPA use case, allowing traffic initiated from remote users (VPN users, secure web gateway (SWG) users, edge devices) to SPA hubs (or local networks behind SPA hubs).

For details on SPA server-to-client communication, see Configuring a private access policy for server-to-client traffic on page 43.

To configure a private access policy from remote VPN users and edge devices to SPA hubs:

1. Go to **Configuration > Policies**.
2. Click the **Private Access** tab and then click the **To hubs** subtab.
3. Click **+Create** to create a new policy.

4. Configure these fields:

Field	Value
Name	Enter a unique private access policy name.
Source Scope	• **All**: all FortiSASE VPN users and edge devices • **VPN Users**: remote endpoint users • **Edge Device**: Edge devices such as FortiExtender
Source	• **All Edge Devices**: Applies to all edge devices • **Specify**: specify selected hosts and host groups if you selected **VPN Users**, or authorized Edge devices if you selected **Edge Device**.
User	• **Specify**: specify selected users and user groups for all source scopes • **Captive Portal Exempt**: If **Source Scope** is set to **Edge Device**, exempt the edge device traffic from encountering a captive portal to determine the identity of a connected endpoint. By default, a captive portal is enforced when edge device traffic matches policies with **Source Scope** set to **All**.
Destination	• **Private Access Traffic**: all private access traffic • **Specify**: specify selected private access hosts or host groups
Service	Click **+** and select services or service groups.
Action	**Accept** or **Deny**
Profile Group	**Default** or **Specify** and select a profile group.
Force Certificate Inspection	Enabled or disabled. When enabled, this policy ignores the SSL inspection mode defined in the selected profile group and instead uses certificate inspection.
Schedule	Select **always** or another recurring schedule.
Status	Enable or disable.
Log Allowed Traffic	Enable or disable. • **Security Events**: log traffic that has a security profile applied to it. • **All Sessions**: log all sessions that this policy accepts or denies.
Comments	Enter comments up to the listed maximum number of characters.

5. Click **OK**.

To configure a private access policy from SWG users to SPA hubs:

1. Go to **Configuration > SWG Policies**.
2. Click the **Private Access** tab and then click the **To hubs** subtab.
3. Click **+Create** to create a new policy.

4. Configure these fields:

Field	Value
Name	Enter a unique private access policy name.
Source Scope	• **All**: all HTTP and HTTPS traffic from SWG users • **Specify**: specify selected hosts and host groups
User	• **All Secure Web Gateway Users**: All SWG users • **Specify**: specify selected users or users groups
Destination	• **Private Access Traffic**: all private access traffic • **Specify**: specify selected private access hosts or host groups
Action	**Accept** or **Deny**
Profile Group	**Default** or **Specify** and select a profile group.
Force Certificate Inspection	Enabled or disabled. When enabled, this policy ignores the SSL inspection mode defined in the selected profile group and instead uses certificate inspection.
Schedule	Select **always** or another recurring schedule.
Status	Enable or disable.
Log Allowed Traffic	Enable or disable. • **Security Events**: log traffic that has a security profile applied to it. • **All Sessions**: log all sessions that this policy accepts or denies.
Comments	Enter comments up to the listed maximum number of characters.

5. Click **OK**.

Considerations

- For SSL VPN remote users, whenever changes are made to an existing Internet Access or Private Access policy, they take effect only after SSL VPN users reconnect to FortiSASE.
- With the addition of support for identity-based policies for edge devices in FortiSASE 24.3.a, the behaviour of edge device traffic based on policies has changed in existing FortiSASE instances:
  - Any policies you created before FortiSASE 24.3.a, specifically for edge devices, namely, policies with **Source Scope** set to **Edge Devices** will have **User** set to **Captive Portal Exempt**.
  - Any policies you created before FortiSASE 24.3.a with **Source Scope** set to **All** will not be modified. Therefore, any edge devices whose traffic matched an **All** allow policy before will now have authentication enforced using the captive portal. You must explicitly create a new exemption policy and place it above any **All** allow policies to avoid captive portal authentication for any impacted edge devices. See Configuring an exemption policy for an edge device.
- When SSO authentication is used with the captive portal for edge devices, you must add an exemption policy for the SAML IdP URLs specified using hosts or infrastructure selections for the Destination field to allow SSO authentication traffic destined for the IdP to bypass the captive portal. See Configuring an exemption policy for SSO authentication for Entra ID.

Configuring a private access policy for server-to-client traffic

Secure private access (SPA) server-to-client communication allows traffic initiated from SPA hubs (or local networks behind SPA hubs) to remote users (currently VPN users only). This communication requires the Remote VPN and edge device user identification feature and additional configuration steps on the FortiGate SPA hub itself. See Prerequisites and considerations on page 44.

For details on SPA client-to-server communication, see Configuring a private access policy for client-to-server traffic on page 40.

To configure a private access policy to remote users from SPA hubs:

1. Go to **Configuration > Policies**.
2. Click the **Private Access** tab and then click the **From hubs** subtab.
3. Click **+Create** to create a new policy.
4. Configure these fields:

Field	Value
Name	Enter a unique private access policy name.
Source Scope	• **Private Access Traffic**: all private access traffic • **Specify**: specify selected private access hosts or host groups.
Destination	• **All**: all FortiSASE users/devices • **VPN Users**: remote endpoint users
Service	Click **+** and select services or service groups.
Action	**Accept** or **Deny**
Profile Group	**Default** or **Specify** and select a profile group.
Force Certificate Inspection	Enabled or disabled. When enabled, this policy ignores the SSL inspection mode defined in the selected profile group and instead uses certificate inspection.
Schedule	Select **always** or another recurring schedule.
Status	Enable or disable.
Log Allowed Traffic	Enable or disable. • **Security Events**: log traffic that has a security profile applied to it. • **All Sessions**: log all sessions that this policy accepts or denies.
Comments	Enter comments up to the listed maximum number of characters.

5. Click **OK**.

To configure a FortiGate SPA hub firewall policy required for traffic from SPA hubs:

On the FortiGate SPA hub, you must configure a firewall policy allowing traffic from the desired local interface(s) or spokes behind the hub to the remote VPN and edge device users via the SPA overlay. This policy ensures that traffic from networks connected to the FortiGate SPA hub are allowed to FortiSASE remote VPN and edge device users.

In this example, for the FortiGate SPA hub, the SPA overlay (IPsec VPN tunnel) is defined as **fgt_hub1** and the local connected networks DMZ_HQ and LAN_HQ are on port2 and port4, respectively. Therefore, we create a policy that allows traffic from the local connected networks on the hub to the FortiSASE remote VPN users.

1. On the FortiGate SPA hub, go to **Policy & Objects > Firewall Policy**.
2. Click **+Create New** to create a new policy.
3. Configure these fields:

Field	Value
Name	Enter a unique private access policy name.
Incoming Interface	*DMZ_HQ (port2)* *LAN_HQ (port4)*
Outgoing Interface	*fgt_hub1*
Source	*all*
Destination	*All*
Schedule	*always*
Service	*ALL*
Action	*ACCEPT*
NAT	You can enable or disable NAT depending on the IP configuration of the organization's FortiGate SPA hub.
IP Pool Configuration	*Use Outgoing Interface Address*

4. Click **OK**.

Prerequisites and considerations

Prerequisites

- The display of the **From hubs** subtab and resulting functionality requires a FortiSASE instance with the remote VPN user identification feature, which is included with new instances created after the FortiSASE 24.3.b release and may need to be added on instances created before that release. See Remote VPN and edge device user identification. Otherwise, the **From hubs** subtab does not display.
- Currently, FortiSASE supports traffic from SPA hubs to remote VPN users only.
- On the FortiGate SPA hub, you must configure a firewall policy allowing traffic from the desired local interface(s) or spokes behind the hub to the remote VPN users via the SPA overlay. This policy ensures that traffic from networks connected to the FortiGate SPA hub are allowed to FortiSASE remote VPN users.

Considerations

- For SSL VPN remote users, whenever changes are made to an existing Internet Access or Private Access policy, they take effect only after SSL VPN users reconnect to FortiSASE.
- With the addition of support for identity-based policies for edge devices in FortiSASE 24.3.a, the behaviour of edge device traffic based on policies has changed in existing FortiSASE instances:
  - Any policies you created before FortiSASE 24.3.a, specifically for edge devices, namely, policies with **Source Scope** set to **Edge Devices** will have **User** set to **Captive Portal Exempt**.
  - Any policies you created before FortiSASE 24.3.a with **Source Scope** set to **All** will not be modified. Therefore, any edge devices whose traffic matched an **All** allow policy before will now have authentication enforced using the captive portal. You must explicitly create a new exemption policy and place it above any

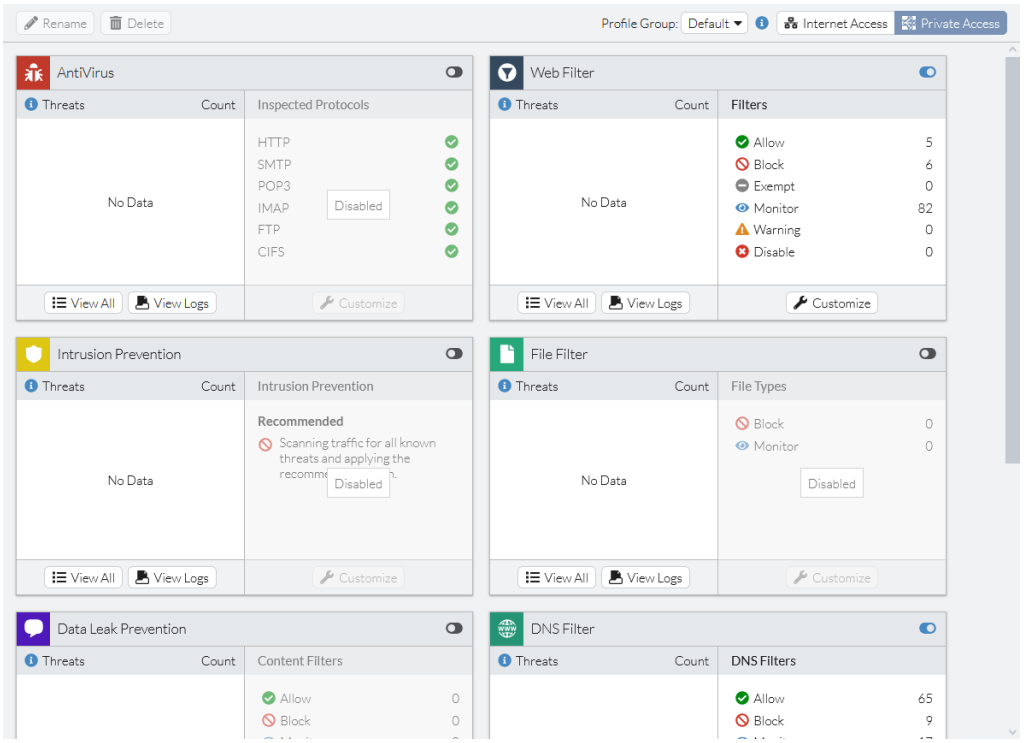
All allow policies to avoid captive portal authentication for any impacted edge devices. See Configuring an exemption policy for an edge device.

- When SSO authentication is used with the captive portal for edge devices, you must add an exemption policy for the SAML IdP URLs specified using hosts or infrastructure selections for the Destination field to allow SSO authentication traffic destined for the IdP to bypass the captive portal. See Configuring an exemption policy for SSO authentication for Entra ID.

Configuring a private access security profile

To configure a private access security profile:

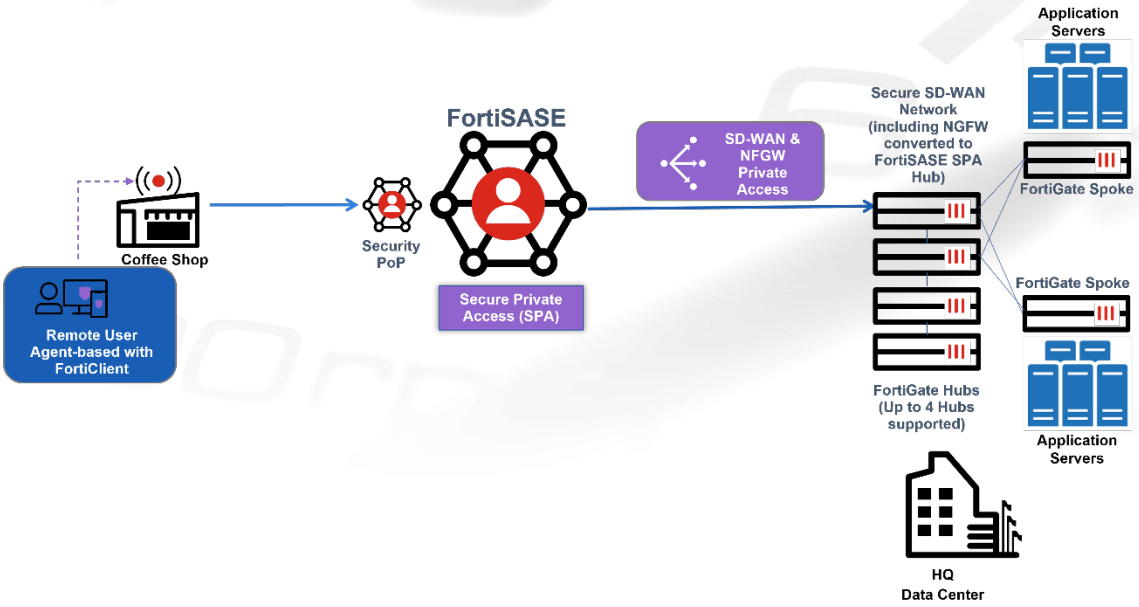
1. Go to *Configuration* > *Traffic* > *Security*.
2. In the top right corner, click *Private Access*.
3. Enable or disable profiles as desired. For enabled security profiles, customize as desired.



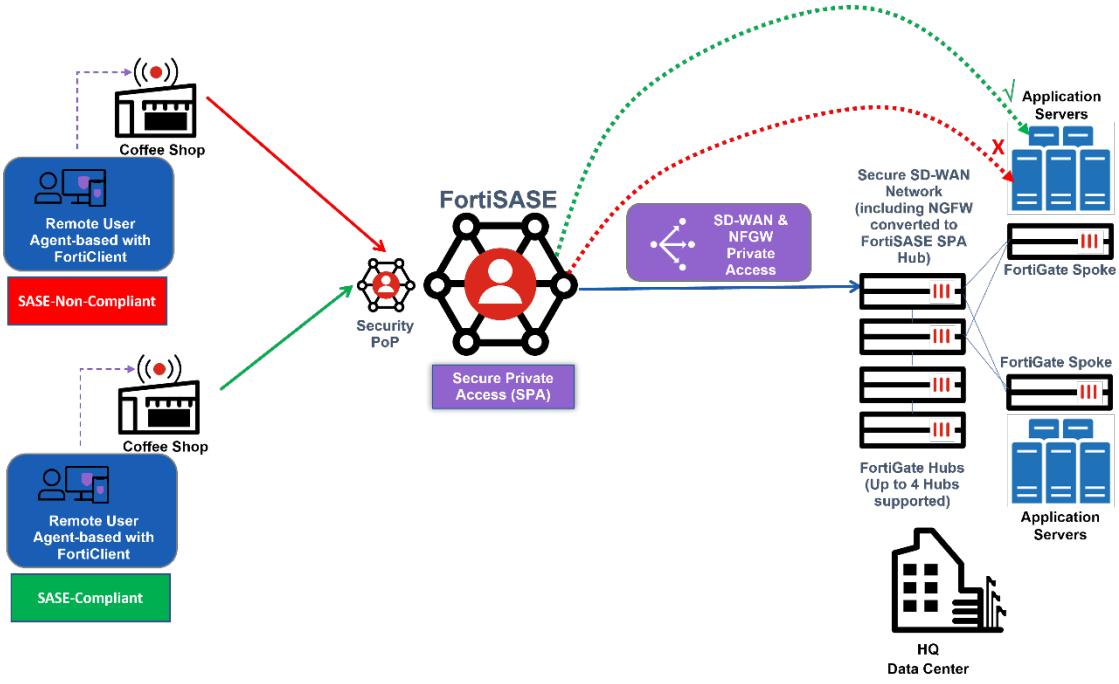
The security settings for Internet and private access are identical. For details on configuring security settings, see Security.

Configuring ZTNA tags in private access policies

By default, for the secure private access (SPA) use cases using a FortiGate hub configured through the *Private Access* page, all FortiSASE agent-based remote users have unrestricted access to private applications behind the hub network through an Allow-All Private Traffic private access policy.



To restrict SPA to private applications of any protocol (TCP, UDP, ICMP, and so on) behind a FortiGate hub, in the FortiSASE portal you can configure zero trust network access (ZTNA) tagging rules that apply ZTNA tags to remote users based on specified endpoint posture checks. You can then specify these tags as the source in a dynamic private access policy to deny or allow access as desired.



Using ZTNA tags to configure dynamic policies

You can use tags to build dynamic policies that you do not need to manually reconfigure whenever an endpoint's status changes. For example, consider that you want to deny Windows endpoints without antivirus (AV) installed and running as detected by FortiClient from accessing private applications behind the FortiGate hub. You would configure the following:

- Rule that applies a SASE-Compliant tag to Windows endpoints that FortiClient detects as having AV software installed and running

- Rule that applies a SASE-Non-Compliant tag to Windows endpoints that FortiClient detects as not having AV software installed
- Private access policy that allows Windows endpoints with the SASE-Compliant tag to access a specific server behind the FortiGate hub
- Private access policy that denies Windows endpoints with the SASE-Non-Compliant tag from accessing a specific server behind the FortiGate hub

As FortiSASE receives information from endpoints, it dynamically removes and applies the SASE-Non-Compliant tag to endpoints. For example, if an endpoint that previously had the SASE-Non-Compliant tag applied has its AV software installed or enabled as detected by FortiClient, then FortiSASE automatically removes the SASE-Non-Compliant tag from the endpoint and applies the SASE-Compliant tag instead. Consequently, the endpoint would then be able to access private applications behind the FortiGate hub.

Therefore, a dynamic policy is a policy that has one or more zero trust network access tags specified as its source.

For details on configuring dynamic tags and policies, see Tagging.

Configuration workflow

You can follow this configuration workflow, which the document describes in detail using the example configuration of a dynamic private access policy that allows access to private applications, which in this example is a private server behind the FortiGate hub:

1. Configure a zero trust network access (ZTNA) tagging rule set for compliant endpoints.
2. Configure a ZTNA tagging rule set for non-compliant endpoints.
3. Configure a dynamic private access policy to allow access to a specific private server from compliant endpoints.
4. Configure a dynamic private access policy to deny access to a specific private server from non-compliant endpoints.
5. Test the dynamic private access policies using ICMP ping to the specific private server from a compliant endpoint and from a non-compliant endpoint, respectively.

A similar workflow applies to a private access policy that allows or denies access to applications of any other protocols besides ICMP, such as TCP or UDP applications.

Configuring ZTNA rule sets to dynamically tag agent-based remote users

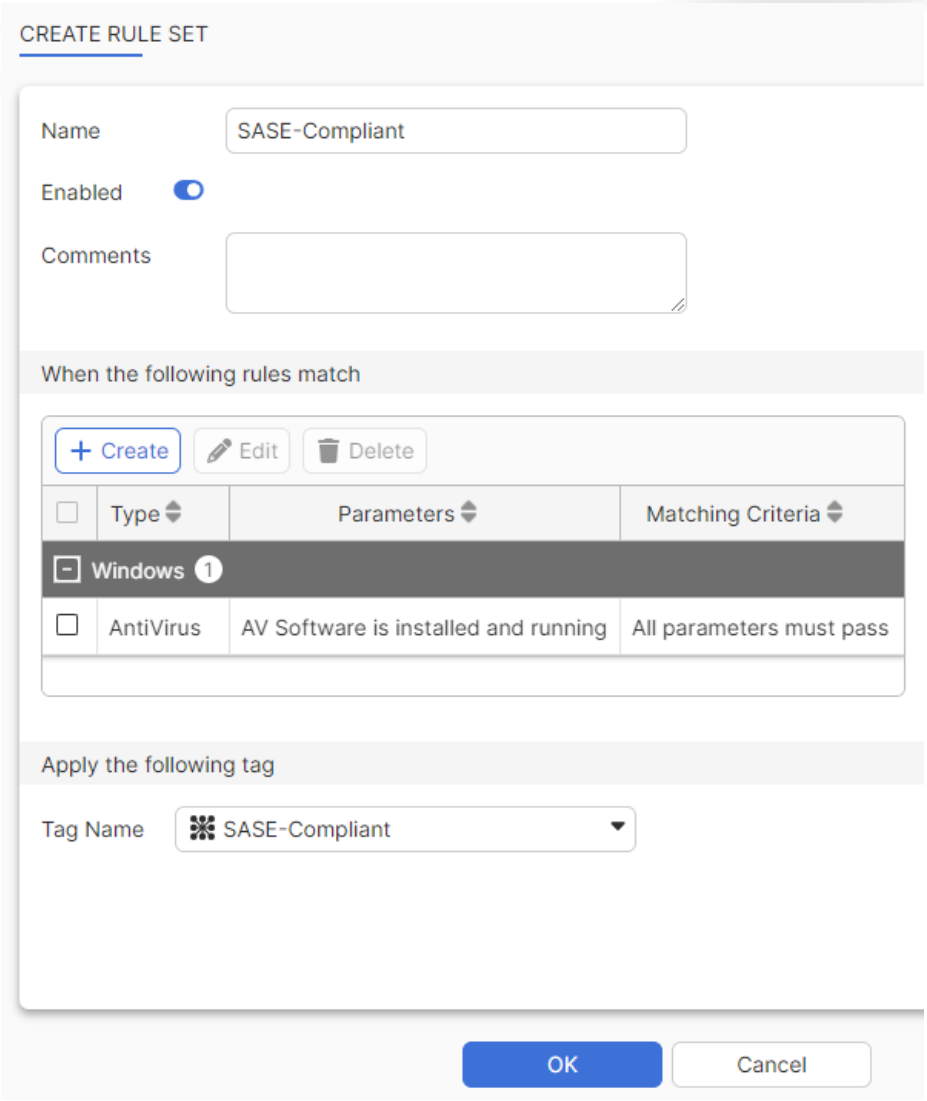
This example demonstrates how to configure zero trust network access (ZTNA) tag names and tagging rule sets with the following posture checks:

- Endpoint is running Windows and has antivirus (AV) software installed and running
- Endpoint is running Windows and does not have AV software installed or running

To configure a ZTNA tagging rule set for compliant endpoints:

1. Go to *Configuration* > *ZTNA Tagging*, and click *Create*.
2. In the *Name* field, enter the desired rule set name. For example, SASE-Compliant.
3. Toggle *Enabled* on or off to enable or disable the rule.
4. (Optional) In the *Comments* field, enter any desired comments.
5. Under *When the following rules match*, click *Create*.

6. Configure the rule:
   a. For *Operating System*, select *Windows*.
   b. From the *Rule Type* dropdown list, select *AntiVirus*.
   c. From the *AntiVirus* dropdown list, select *AntiVirus Software is installed and running*.
   d. Click *OK*.
7. In the *Tag Name* dropdown list, create a tag named SASE-Compliant.
8. Click *OK*.



To configure a ZTNA tagging rule set for non-compliant endpoints:

1. Go to *Configuration* > *ZTNA Tagging*, and click *Create*.
2. In the *Name* field, enter the desired rule set name. For example, SASE-Non-Compliant.
3. Toggle *Enabled* on or off to enable or disable the rule.
4. (Optional) In the *Comments* field, enter any desired comments.
5. Under *When the following rules match*, click *Create*.
6. Configure the rule:
   a. For *Operating System*, select *Windows*.
   b. From the *Rule Type* dropdown list, select *AntiVirus*.
   c. Select *Negate*.

   d. From the *AntiVirus* dropdown list, select *AntiVirus Software is installed and running*.
   e. Click *OK*.
7. In the *Tag Name* dropdown list, create a tag named SASE-Compliant.
8. Click *OK*.

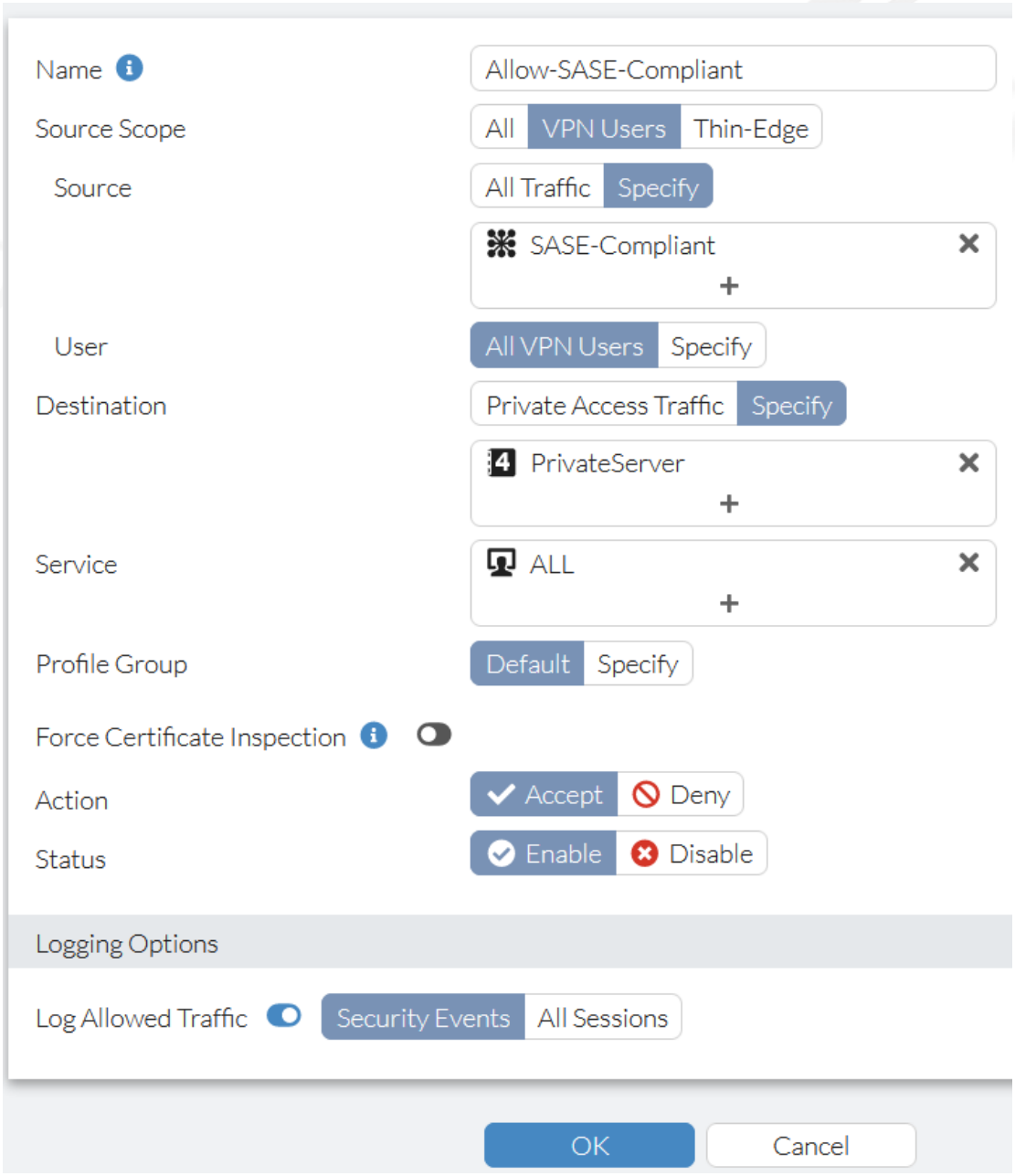
Configuring dynamic private access policies using ZTNA tags

This example demonstrates how to configure dynamic private access policies using the zero trust network access (ZTNA) tags that you created in Configuring ZTNA rule sets to dynamically tag agent-based remote users on page 47 to allow endpoints tagged as SASE-Compliant with access to selected private resources and to deny access to selected private resources for endpoints tagged as SASE-Non-Compliant.

To configure a dynamic private access policy for compliant endpoints:

1. Go to *Configuration* > *Policies*.
2. Select *Private Access* to display the list of private access policies
3. Click *Create*.
4. Configure the policy:
   a. For *Name*, enter Allow-SASE-Compliant.
   b. For *Source Scope*, select *VPN Users*.
   c. In the *Source* field, select *Specify* and click *+*. From the *Select Entries* panel, under *ZTNA Tag* > *Private Access*, select the *SASE-Compliant* tag.
   d. For *Destination*, select *Specify*, click *+*, and in the *Select Entries* panel click *+Create* and click *IPv4 Host* to a create a new host for the specific server as follows:
      i. For *Location*, select *Private Access Hub*.
      ii. For *Category*, *IPv4 Host* is selected.
      iii. In the *Name* field, enter the desired name. In this example, the name is PrivateServer.
      iv. From the *Type* dropdown list, select *Subnet*.
      v. In the *IP/Netmask* field, enter 10.100.99.101/32.
      vi. Click *OK*.
      Select the newly created host to set it as the *Destination*.
   e. For *Service*, click *+* and from the *Select Entries* panel select *ALL*.
   f. For *Action*, select *Accept*.
   g. For *Status*, select *Enable*.

5. Click *OK*.



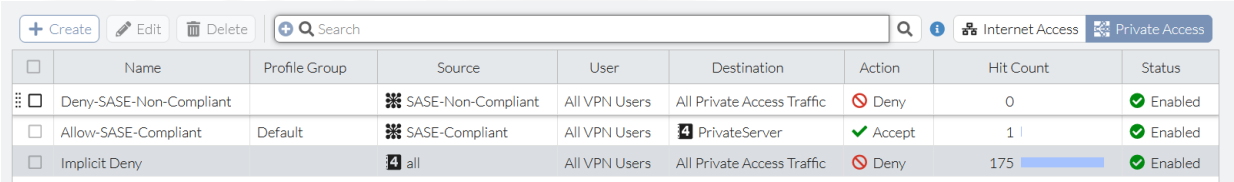
6. In *Configuration* > *Policies* with *Secure Private Access* selected, ensure that you order the policies so that the Allow-SASE-Compliant policy is before the Allow-All Private Traffic policy. With this ordering of policies, FortiSASE allows endpoints that match the dynamic policy access to the specific private server.

To configure a dynamic private access policy for non-compliant endpoints:

1. Go to *Configuration* > *Policies*.
2. Select *Private Access* to display the list of private access policies
3. Click *Create*.
4. Configure the policy:
   a. For *Name*, enter Deny-SASE-Non-Compliant.
   b. For *Source Scope*, select *VPN Users*.
   c. In the *Source* field, select *Specify* and click *+*. From the *Select Entries* panel, under *ZTNA Tag* > *Private Access*, select the *SASE-Non-Compliant* tag.

d. For *Destination*, select *Private Access Traffic*.
e. For *Service*, click + and from the *Select Entries* panel select *ALL*.
f. For *Action*, select *Deny*.
g. For *Status*, select *Enable*.

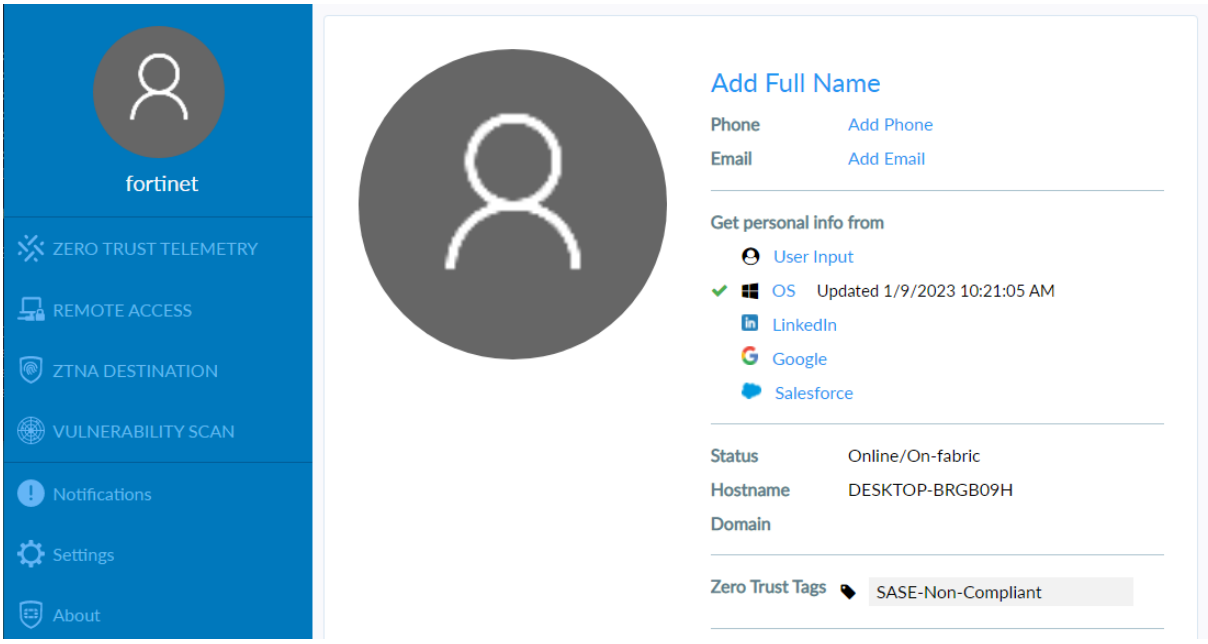
5. Click *OK*.
6. In *Configuration* > *Policies* with *Secure Private Access* selected, do the following:
   a. Ensure that you order the policies so that the Allow-SASE-Compliant policy is before the Allow-All Private Traffic policy. With this ordering of policies, FortiSASE allows endpoints that match the dynamic policy access to the specific private server.
   b. Delete the Allow-All Private Traffic and Allow-All Private Traffic Thin edge policies.



Testing the dynamic private access policy

(Optional) To display tags on the FortiClient endpoint:

1. In FortiSASE, go to *Configuration* > *Endpoints* > *Profile*.
2. Enable *Show tags on FortiClient*.
3. Click *Apply*. When this option is enabled, detected tags appear on the FortiClient avatar page.



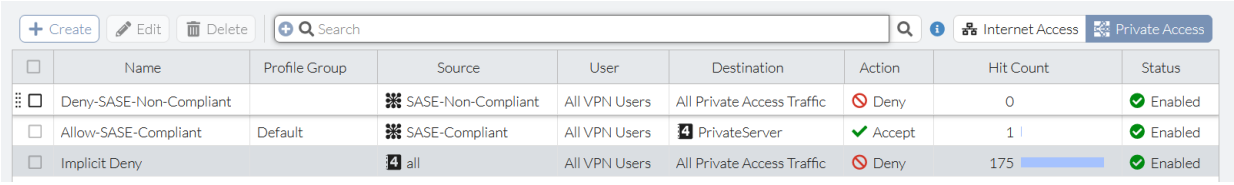
To test that FortiSASE allows a FortiClient endpoint tagged as SASE-Compliant access to a private server:

1. In FortiClient, go to the *REMOTE ACCESS* tab.
2. From the *VPN Name* dropdown list, select *Secure Internet Access*.
3. Enter the user credentials based on the VPN user authentication defined on FortiSASE. Click *Connect*.
4. In Windows Defender, set *Real-time protection* to *On* as Stay protected with Windows Security describes. This turns on antivirus (AV) and ensures that FortiSASE dynamically tags the endpoint as compliant.

5. From the FortiClient avatar page, ensure that the endpoint is non-compliant and has the SASE-Compliant Zero Trust tag applied.
6. In Windows Command Prompt, enter `ping 10.100.99.101` to test an ICMP ping to the specified private server with IP address 10.100.99.101 behind the FortiGate hub.
7. Observe the following output indicating the ping succeeded since FortiSASE allows access:

```
C:\> ping 10.100.99.101

Pinging 10.100.99.101 with 32 bytes of data:
Reply from 10.100.99.101: bytes=32 time=137ms TTL=62
Reply from 10.100.99.101: bytes=32 time=137ms TTL=62
Reply from 10.100.99.101: bytes=32 time=137ms TTL=62
Reply from 10.100.99.101: bytes=32 time=136ms TTL=62

Ping statistics for 10.100.99.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 136ms, Maximum = 137ms, Average = 136ms
```

8. In FortiSASE, in *Configuration* > *Policies*, observe that the Allow-SASE-Compliant dynamic private access policy hit count increased and that the Deny-SASE-Non-Compliant dynamic private access policy hit count has not changed.



To test that FortiSASE denies a FortiClient endpoint tagged as SASE-Non-Compliant access to a private server:

1. In FortiClient, go to the *REMOTE ACCESS* tab.
2. From the *VPN Name* dropdown list, select *Secure Internet Access*.
3. Enter the user credentials based on the VPN user authentication defined on FortiSASE. Click *Connect*.
4. In Windows Defender, set *Real-time protection* to *Off* as Stay protected with Windows Security describes. This turns off AV and ensures that FortiSASE dynamically tags the endpoint as non-compliant.
5. From the FortiClient avatar page, ensure that the endpoint is non-compliant and has the SASE-Non-Compliant Zero Trust tag applied.
6. In Windows Command Prompt, enter `ping 10.100.99.101` to test an ICMP ping to the specified private server with IP address 10.100.99.101 behind the FortiGate hub.
7. Observe the following output indicating the ICMP ping has timed out since FortiSASE denies access to the specific server:

```
C:\> ping 10.100.99.101

Pinging 10.100.99.101 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.100.99.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

8. In FortiSASE, in *Configuration* > *Policies*, observe that the Allow-SASE-Compliant dynamic private access policy hit count has not changed and that the Deny-SASE-Non-Compliant dynamic private access policy hit count increased.

Configuring DNS Settings

Agent-based remote users use the *VPN Implicit DNS Rule* setting in FortiSASE under *Configuration* > *DNS* to resolve hostnames for internal and external domains.

By default, FortiSASE deployments use FortiGuard DNS as the default DNS server.

You can configure the *VPN Implicit DNS Rule* with one of the following options and then click *OK* to save the change:

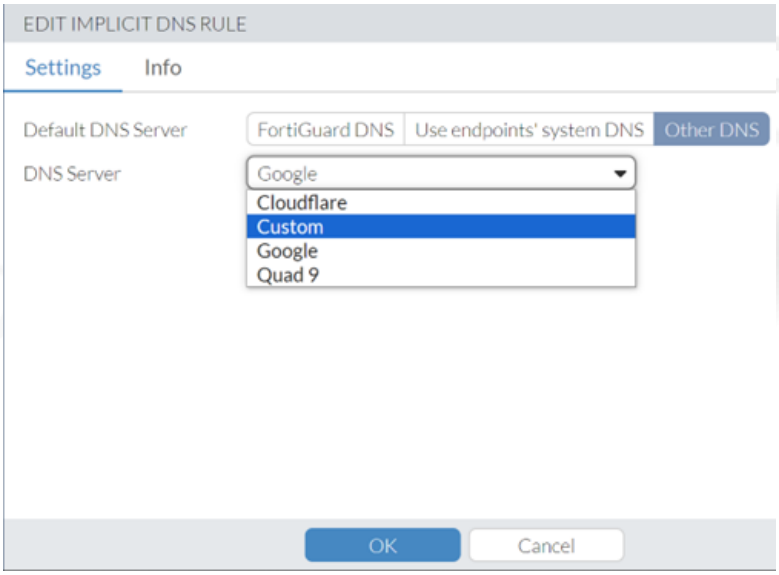
DNS Server		Description	Primary and Secondary DNS Server IP Address
FortiGuard DNS		Use FortiGuard DNS	208.91.112.53 208.91.112.52
Use endpoints' system DNS		Use the system DNS setting already configured on the agent-based endpoints	IP addresses specific to endpoints
Other DNS		Use a public DNS server other than FortiGuard DNS	IP addresses specific to public DNS server
	CloudFlare	Use the CloudFlare public DNS server	1.1.1.1 1.0.0.1
	Custom	Enable to specify your own custom primary and secondary DNS servers..	Specify IP address of primary and secondary DNS.
	Google	Use the Google public DNS server	8.8.8.8 8.8.4.4
	Quad 9	Use the Quad 9 public DNS server	9.9.9.9 149.112.112.112

For example, you can edit the VPN implicit DNS rule to use a custom DNS server as follows:

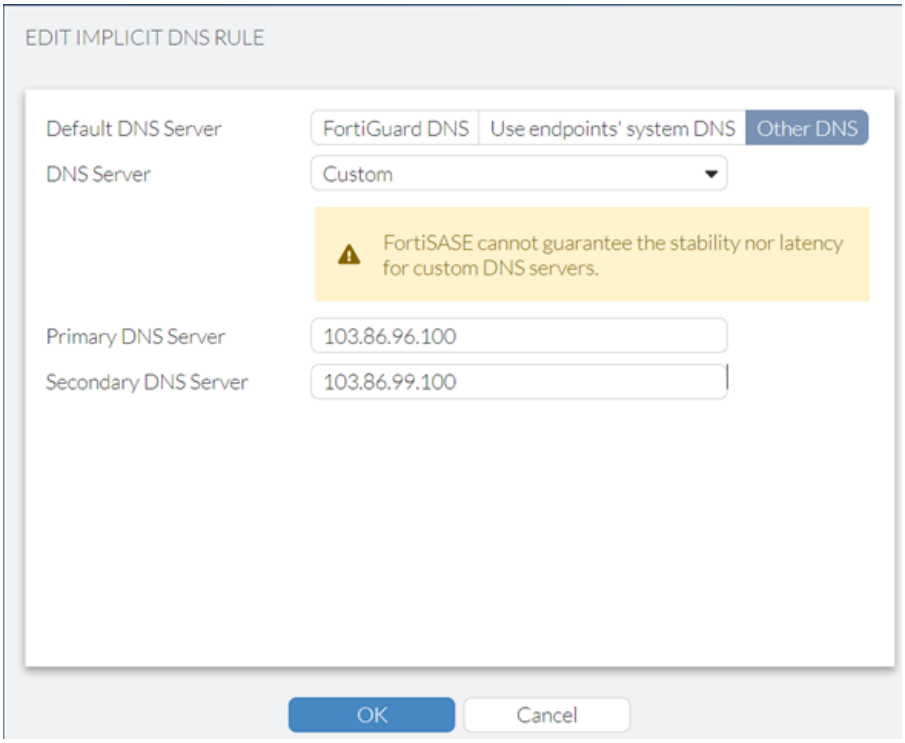
To configure a custom DNS server:

1. Go to *Configuration* > *DNS*, select *VPN Implicit DNS Rule*, and click *Edit*.
2. In the *Edit Implicit DNS Rule* page, for *Default DNS Server*, select *Other DNS*.

3. From the *DNS Server* dropdown, select *Custom*.



4. In the *Primary DNS Server* and *Secondary DNS Server* fields, enter the respective IP addresses for the servers of your choice.



5. Click *OK*.

Using FortiGuard DNS or another public DNS service is sufficient for most agent-based Secure Internet Access (SIA) use cases that simply require agent-based remote users to resolve hostnames for external domains.

Split DNS Rules

FortiSASE agent-based users often must resolve internal hostnames that public DNS servers cannot resolve in scenarios including but not limited to:

- When users are located within the organization's local network, also known as being on-net, and users must use an internal DNS server instead of a public DNS server.
- When users are located remotely, FortiSASE Private Access has been configured with Secure Private Access (SPA) hubs, and users must use an internal DNS server behind the SPA hub.

To support these scenarios,FortiSASE DNS settings can be configured for split DNS using *Split DNS Rules*.

Split DNS works as follows:

- Selectively use an internal DNS server only when it is necessary to resolve hostnames for the specified internal domain(s).
- Resolve all other hostnames for external domains using the implicit DNS rule.

Split DNS is more efficient than sending all DNS requests to internal DNS servers because it reduces any potential latency and downtime with using internal DNS servers for resolving public hostnames if any issues arise with these limited availability and limited resource internal DNS server deployments. For resolving hostnames for external domains, split DNS leverages the redundancy, extensive resources, and geographical coverage of public DNS servers with anycast capabilities.

For the scenario with on-net users who must use an internal DNS server to resolve hostnames for the internal domain, configuring split DNS using an internal DNS server with a private IP address and without an SPA hub configured in FortiSASE yields inconsistent results. When an SPA hub is not configured in FortiSASE, ensure that split DNS is configured using an internal DNS server with a public IP address.

Split DNS supports using an internal DNS server with a private IP address only when an SPA hub is configured in FortiSASE.

To secure DNS requests, the DNS-over-HTTPS (DoH) protocol secures DNS requests and replies sent and received over HTTPS and works with public DNS servers that support this protocol. DoH is enabled by default on modern web browsers including Chrome, Edge, and Firefox and is supported by Google's public DNS servers, which is the default for upgraded FortiSASE deployments. Therefore, for split DNS rules to work with DNS servers that support DoH, SSL deep inspection must be enabled for agent-based remote users on FortiSASE.

Prerequisites

SSL Deep Inspection

Split DNS requires SSL deep inspection to be enabled on FortiSASE so that FortiSASE can intercept the DNS traffic.

- To confirm SSL deep inspection is enabled, go to *Configuration* > *Security* and under the *SSL Inspection* widget ensure *Deep Inspection* is displayed.
- To enable SSL deep inspection, go to *Configuration* > *Security* and in the *SSL Inspection* widget click on *Customize*. In the *SSL Inspection* pane, select *Deep Inspection* and click *OK*.

See Certificate and deep inspection modes for further details on deep inspection.

Access to Internal DNS Server

Ensure that your FortiSASE remote users have access to the internal DNS server.

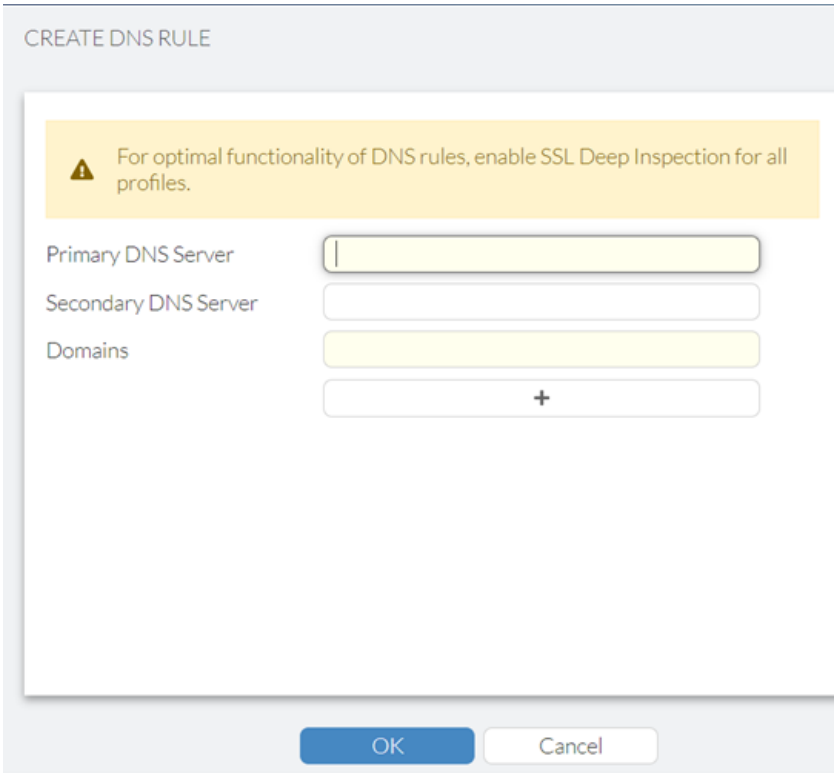
For the scenario with on-net users who must use an internal DNS server to resolve hostnames for the internal domain, configuring split DNS using an internal DNS server with a private IP address and without an SPA hub configured in FortiSASE yields inconsistent results. When an SPA hub is not configured in FortiSASE, ensure that split DNS is configured using an internal DNS server with a public IP address.

Split DNS supports using an internal DNS server with a private IP address only when an SPA hub is configured in FortiSASE.

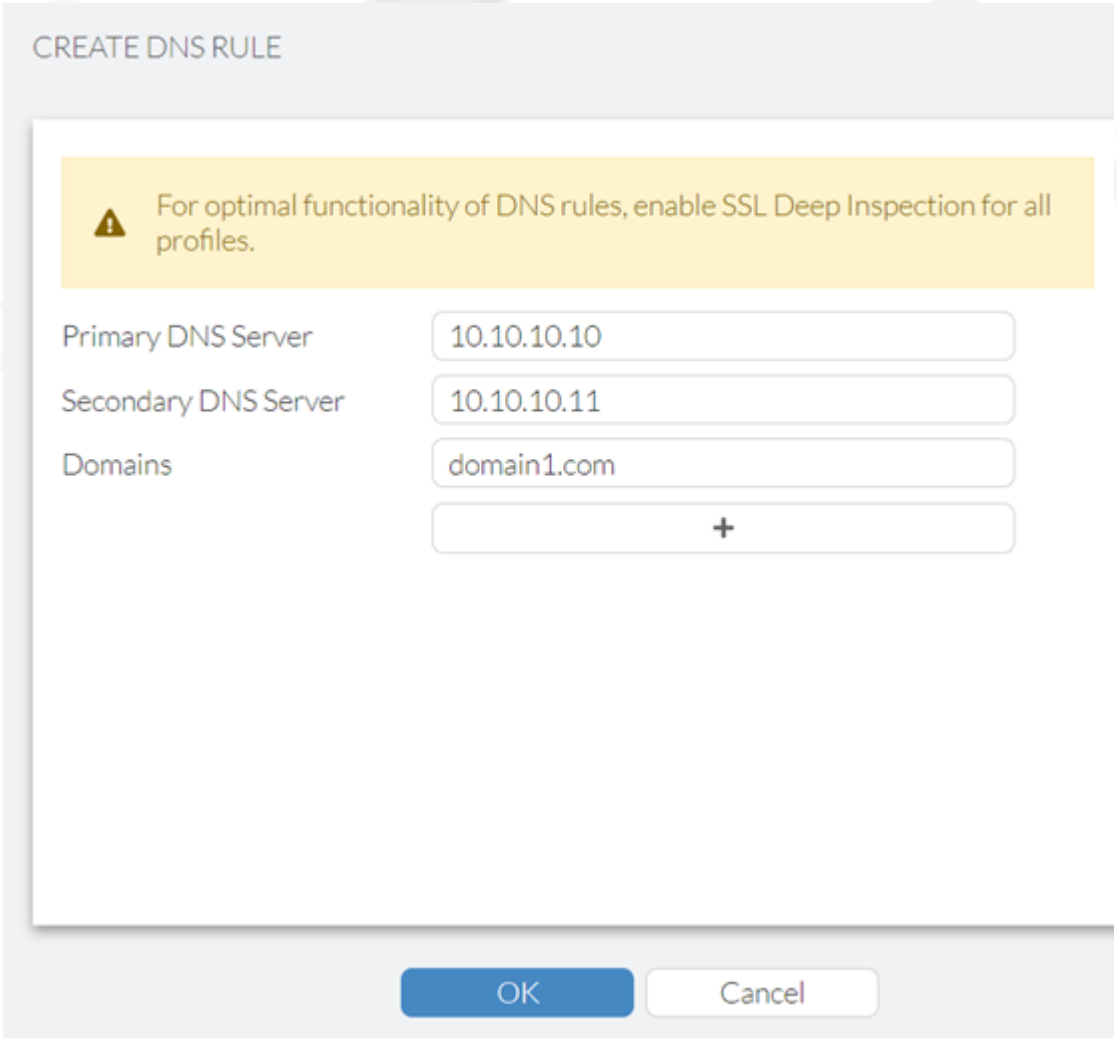
Configuring Split DNS Rules

To configure Split DNS Rules:

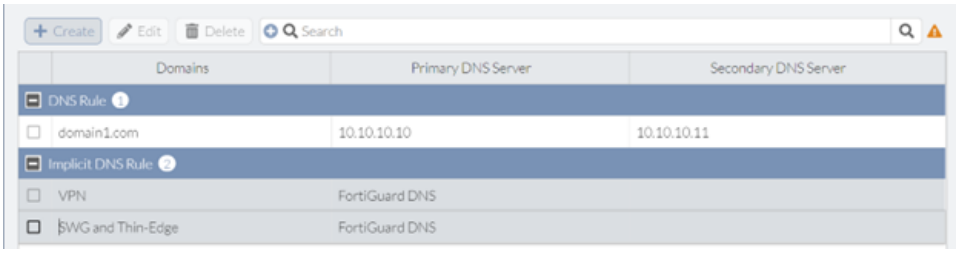
1. Go to *Configuration* > *DNS*.
2. Click *Create*.



3. In the *Create DNS Rule* pane, enter the *Primary DNS Server*, (optional) *Secondary DNS Server*, and one or more *Domains*. Click + to add more fields to enter in additional domains. Click *OK*.



4. Observe that the split DNS rule has been created and is displayed in the table.



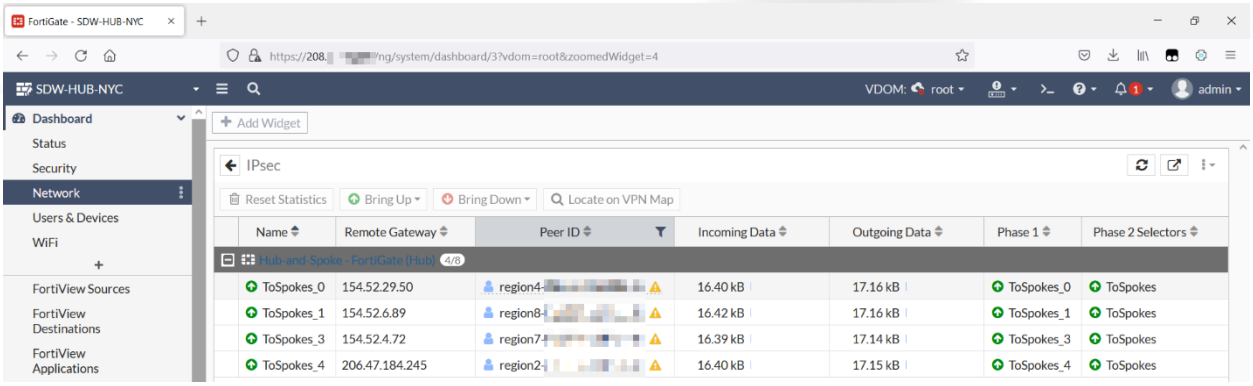
If you are using split DNS to resolve local domains using an internal DNS server with an SPA hub configured, then the Web Filter or DNS Filter blocks access to these local domains from FortiClient remote users if the Newly Observed Domain category is set to Block in the respective security component. In this case, you must create URL Filter entries for the Web Filter or Domain Filter entries for the DNS Filter to allow access to these local domains.

If you are using split DNS to resolve local domains using an internal DNS server with an SPA hub configured, to ensure access to the internal DNS server from FortiClient remote users you must have a Private Access policy configured that allows DNS requests to that specific server.

Verifying IPsec VPN tunnels on the FortiGate hub

Verify that the IPsec VPN tunnels immediately appear on the FortiGate hub from all configured FortiSASE security points of presence(PoP).

On the FortiGate hub, verify that the IPsec VPN tunnels from the FortiSASE PoPs acting as spokes by going to *Dashboard* > *Network* and clicking the *IPsec* widget to expand it.



To verify IPsec VPN tunnels using the CLI:

1. Run at least one of the following commands. For a VDOM-enabled hub FortiGate, enter the proper VDOM before running the command(s):
   diagnose vpn ike gateway list
   diagnose vpn tunnel list
   get vpn ipsec tunnel summary
   a. For `diagnose vpn ike gateway list`, confirm that the phase 1 IKE security associations (SA) for the FortiSASE security PoPs with corresponding peer IDs are established. Confirm that the IKE SA and IPsec VPN SA show created and established as 1/1. The following shows sample output for this command:

```
vd: root/0
name: ToSpokes_1
version: 2
...
created: 923s ago
peer-id: region8-fos001-tiui7pzu-1
...
IKE SA: created 1/1  established 1/1  time 10/10/10 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms


 ...
 direction: responder
 status: established 923-923s ago = 10ms
 proposal: aes128-sha256
 child: no
 ...
 PPK: no
 message-id sent/recv: 1/2
 lifetime/rekey: 86400/85206
 DPD sent/recv: 00000001/00000001
 peer-id: region8-fos001-tiui7pzu-1
```

2. For `diagnose vpn tunnel list`, confirm that the phase 2 IPsec VPN SAs for the FortiSASE security PoPs are established. Confirm that the SA field exist and are populated. The following shows sample output for this command:

```
name=ToSpokes_1 ver=2 serial=3ba 208.85.68.228:4500->154.52.6.89:52270 tun_id=10.150.160.2 tun_
id6=::10.0.3.147 dst_mtu=1500 dpd-link=on
 weight=1
bound_if=25 lgwy=static/1 tun=intf/2 mode=dial_inst/3 encap=none/9096 options[2388]=npu rgwy-chg rport-
chg frag-rfc  run_state=0 accept_
traffic=1 overlay_id=0
parent=ToSpokes index=1
proxyid_num=1 child_num=0 refcnt=6 ilast=0 olast=0 ad=s/1
stat: rxp=2689 txp=1042 rxb=16418 txb=18338
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=1
natt: mode=silent draft=0 interval=10 remote_port=52270
proxyid=ToSpokes proto=0 sa=1 ref=4 serial=1 ads
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=6 options=a26 type=00 soft=0 mtu=1422 expire=42258/0B replaywin=2048
       seqno=411 esn=0 replaywin_lastseq=00000a80 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43187/43200
  dec: spi=fd64b472 esp=aes key=16 0ab999cd40bc420cc78556f84b37747f
       ah=sha1 key=20 2e9f19e91d696d530adefb3d219ad1c74d08dcd8
  enc: spi=14c9a05c esp=aes key=16 5446e233d666319b8f88fd1768f774b0
       ah=sha1 key=20 15989dc3ef5fd1d0b385df93241e0d6a0b373826
  dec:pkts/bytes=2689/16346, enc:pkts/bytes=1042/21844
  npu_flag=03 npu_rgwy=154.52.6.89 npu_lgwy=208.85.68.228 npu_selid=33d dec_npuid=1 enc_npuid=1
```

3. For `get vpn ipsec tunnel summary`, confirm that the phase 2 IPsec VPN selectors for the FortiSASE security PoPs are sending and receiving traffic. Confirm that `selectors(total,up): 1/1`, `rx(pkt,err)`, and `tx(pkt,err)` are non-zero. The following shows sample output for this command:

```
'ToSpokes_0' 154.52.29.50:64916  selectors(total,up): 1/1  rx(pkt,err): 2689/0  tx(pkt,err): 1043/0
'ToSpokes_1' 154.52.6.89:52270  selectors(total,up): 1/1  rx(pkt,err): 2689/0  tx(pkt,err): 1042/0
'ToSpokes_2' 50.208.126.11:0  selectors(total,up): 1/1  rx(pkt,err): 22149/0  tx(pkt,err): 55050/37
...
'ToSpokes_4' 206.47.184.245:64916  selectors(total,up): 1/1  rx(pkt,err): 2689/0  tx(pkt,err): 1043/0
...
```

Verifying BGP routing on the FortiGate hub

To verify that all BGP peering is up on the FortiGate hub:

1. Check the BGP peering status and the advertised routes using the following CLI commands. Replace x.x.x.x with the BGP neighbor IP address:

   get router info bgp summary

   get router info bgp neighbors x.x.x.x advertised-routes

2. On the GUI, verify routing by going to *Dashboard* > *Networks*. Click the *Static & Dynamic Routing* widget to expand it, then select *BGP Neighbors* from the dropdown list in the top right corner.

Testing private access connectivity to FortiGate hub network from remote VPN users and edge devices

By using ping, you can verify access to the FortiGate hub network from FortiSASE remote users, namely, FortiClient users connected to FortiSASE in FortiClient agent-based mode and users behind FortiSASE edge devices.

For example, from a FortiClient user connected to FortiSASE, use ping within a Windows Command Prompt to verify access to a host behind the FortiGate hub internal network. The example pings 10.50.101.50, which is on an internal network. The following shows sample output:

C:\>ping 10.50.101.50

Pinging 10.50.101.50 with 32 bytes of data:

Reply from 10.50.101.50: bytes=32 time=80ms TTL=62

Reply from 10.50.101.50: bytes=32 time=80ms TTL=62

Reply from 10.50.101.50: bytes=32 time=80ms TTL=62

Reply from 10.50.101.50: bytes=32 time=84ms TTL=62

Testing private access connectivity to FortiGate hub network from remote SWG users

This example requires *System > SWG Configuration* and *Configuration > SWG User SSO* to be configured appropriately. See SWG client onboarding and Configuring FortiSASE with Entra ID SSO in SWG agentless mode.

By default, all SWG users can access all private access resources. You can limit SWG user access to private access resources by creating a private access policy for SWG users. See Configuring a private access policy for SWG users.

You can verify access to the FortiGate hub network from FortiSASE SWG users by using a web browser to access a host on the hub local network.

For example, consider the case when a host on the hub local network has an HTTP server running on 10.100.99.101 and only the default private access policy for SWG users is in place in FortiSASE.

To test private access connectivity to FortiGate hub network from remote SWG users:

1. From a web browser configured for SWG enter http://10.100.99.101.
2. If this is the first time going out to the internet, you will be prompted by SAML SSO to enter your credentials.
3. After entering your credentials, you should be able to access the web site at http://10.100.99.101 .

Testing private access connectivity from FortiGate hub network to remote VPN users

This test depends on a private access policy being defined in the *From Hub* direction on a FortiSASE instance with the remote VPN user identification selected availability feature. See Remote VPN user identification.

You can verify access from the FortiGate hub network to FortiSASE VPN users, namely FortiClient users connected to FortiSASE in FortiClient agent-based endpoint mode using ping.

From a host behind the FortiGate hub internal network, use ping to verify access to a FortiClient user connected to FortiSASE

The example pings the FortiClient user with 100.65.0.1 from 10.100.99.104, which is a host on an internal network. The following shows sample output:

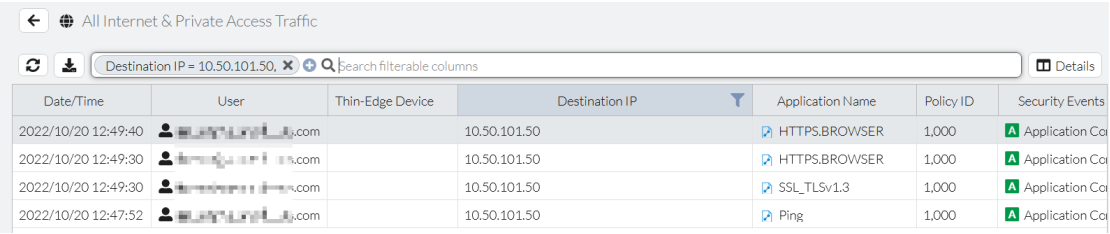
```
root@internal-server-01:~# ping 100.65.0.1
PING 100.65.0.1 (100.65.0.1) 56(84) bytes of data.
64 bytes from 100.65.0.1: icmp_seq=1 ttl=126 time=73.3 ms
64 bytes from 100.65.0.1: icmp_seq=2 ttl=126 time=72.5 ms
64 bytes from 100.65.0.1: icmp_seq=3 ttl=126 time=74.0 ms
64 bytes from 100.65.0.1: icmp_seq=4 ttl=126 time=72.1 ms
^C
--- 100.65.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 72.127/73.008/74.034/0.735 ms
```

Verifying private access traffic in FortiSASE portal

In the FortiSASE portal, you can verify traffic from FortiSASE remote users has reached private access destinations through these methods:

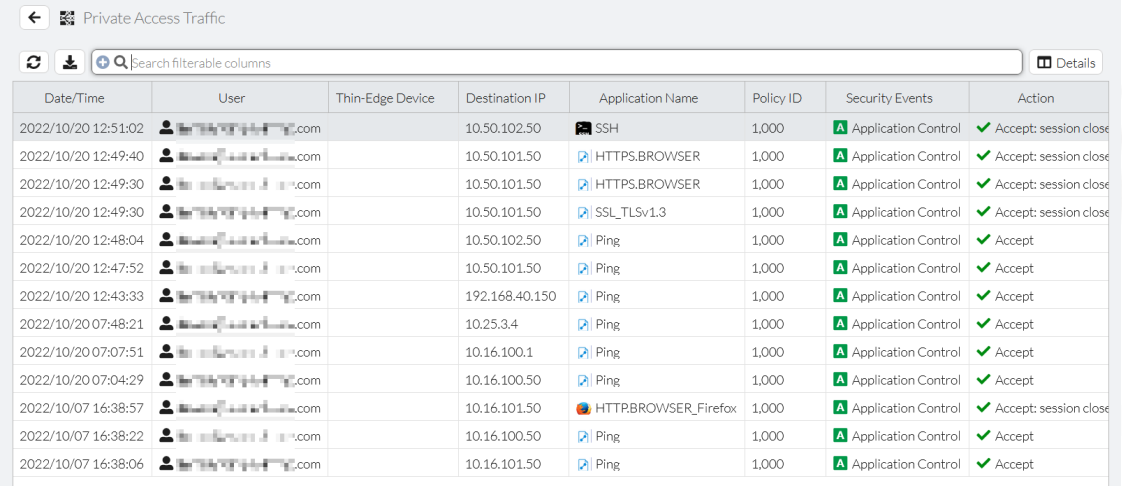
- From *Analytics* > *Logs* > *Traffic* by viewing either the *All Internet and Private Access Traffic* page or the *Private Access Traffic* page
- From *Dashboard* > *FortiView* > *Sources*, *Dashboard* > *FortiView* > *Destinations*, or *Dashboard* > *FortiView* > *Policies* and filtering on the private access destination IP address

Following is an example of the *Analytics* > *Logs* > *Traffic* > *All Internet and Private Access Traffic* page, filtered for the private access destination IP address 10.50.101.50.



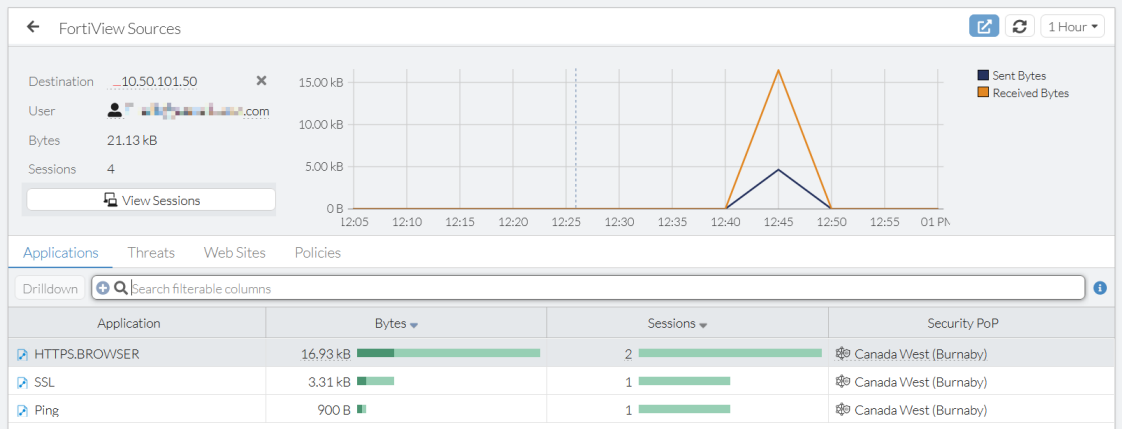
Following is an example of the *Analytics* > *Logs* > *Traffic* > *Private Access Traffic* page.

VERIFYING PRIVATE ACCESS TRAFFIC IN FORTISASE PORTAL



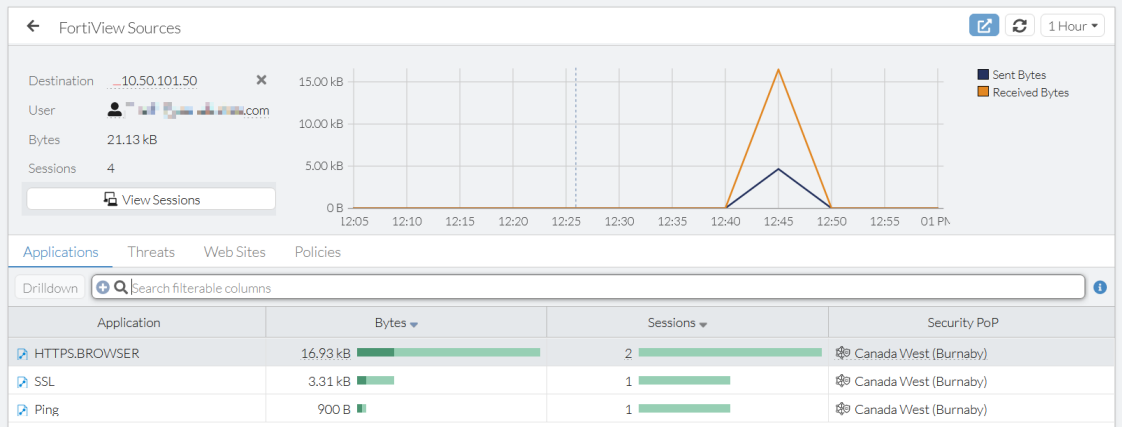
Date/Time	User	Thin-Edge Device	Destination IP	Application Name	Policy ID	Security Events	Action
2022/10/20 12:51:02	[redacted].com		10.50.102.50	SSH	1,000	Application Control	Accept: session close
2022/10/20 12:49:40	[redacted].com		10.50.101.50	HTTPS.BROWSER	1,000	Application Control	Accept: session close
2022/10/20 12:49:30	[redacted].com		10.50.101.50	HTTPS.BROWSER	1,000	Application Control	Accept: session close
2022/10/20 12:49:30	[redacted].com		10.50.101.50	SSL_TLSv1.3	1,000	Application Control	Accept: session close
2022/10/20 12:48:04	[redacted].com		10.50.102.50	Ping	1,000	Application Control	Accept
2022/10/20 12:47:52	[redacted].com		10.50.101.50	Ping	1,000	Application Control	Accept
2022/10/20 12:43:33	[redacted].com		192.168.40.150	Ping	1,000	Application Control	Accept
2022/10/20 07:48:21	[redacted].com		10.25.3.4	Ping	1,000	Application Control	Accept
2022/10/20 07:07:51	[redacted].com		10.16.100.1	Ping	1,000	Application Control	Accept
2022/10/20 07:04:29	[redacted].com		10.16.100.50	Ping	1,000	Application Control	Accept
2022/10/07 16:38:57	[redacted].com		10.16.101.50	HTTP.BROWSER_Firefox	1,000	Application Control	Accept: session close
2022/10/07 16:38:22	[redacted].com		10.16.100.50	Ping	1,000	Application Control	Accept
2022/10/07 16:38:06	[redacted].com		10.16.101.50	Ping	1,000	Application Control	Accept

Following are examples of the *Dashboard* > *FortiView* > *Sources*, *Dashboard* > *FortiView* > *Destinations*, or *Dashboard* > *FortiView* > *Policies* pages, filtered on the private access destination IP address 10.50.101.50.



Application	Bytes	Sessions	Security PoP
HTTPS.BROWSER	16.93 kB	2	Canada West (Burnaby)
SSL	3.31 kB	1	Canada West (Burnaby)
Ping	900 B	1	Canada West (Burnaby)

User	Threat Score	Bytes	Sessions	Security PoP
[redacted].com	0	21.13 kB	4	Canada West (Burnaby)



Verifying private access traffic from hubs

Verifying private access traffic from SPA hubs to FortiSASE remote users depends on a private access policy being defined in the *From Hub* direction on a FortiSASE instance with the remote VPN user identification selected availability feature. See Remote VPN user identification.

In the FortiSASE portal, you can verify traffic from SPA hub sources (local networks or connected spokes) has reached FortiSASE remote user destinations through these methods:

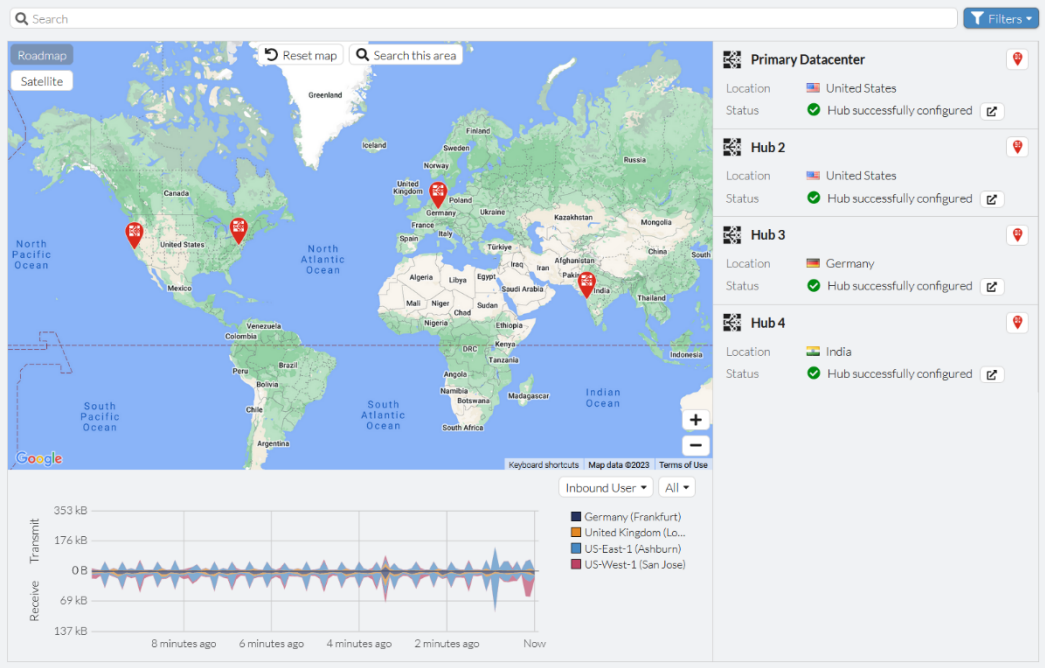
- From *Analytics > Logs > Traffic* by viewing *All Internet and Private Access Traffic* or *Private Access Traffic (From Hubs)*
- From *Dashboard > FortiView > Sources*, *Dashboard > FortiView > Destinations*, or *Dashboard > FortiView > Policies* and filtering on the remote VPN user destination IP address

Verifying private access hub status and location using the asset map

The *Network > Asset Map* page in the FortiSASE portal supports filtering on *Private Access Hub* assets to display their status and geographical location.

Following is an example of the asset map filtered on *Private Access Hub* assets.

VERIFYING PRIVATE ACCESS HUB STATUS AND LOCATION USING THE ASSET MAP



More information

Appendix A: Documentation references

Feature documentation

Product document	Specific chapter if available
FortiOS 7.2.0 Admin Guide	• General IPsec VPN configuration • BGP • ADVPN with BGP as the routing protocol • Firewall policy parameters • Performance SLA • SD-WAN Rules
FortiClient 7.0 Admin Guide	
FortiManager 7.2.1 Admin Guide	• SD-WAN Overlay Templates • IPsec tunnel templates • BGP templates

4-D resources: SASE

- https://docs.fortinet.com/4d-resources/SASE

Appendix C - Converting FortiGate NGFW configured using FortiOS GUI to a FortiSASE SPA hub without using the Fabric Overlay Orchestrator

For ease of configuration, following the steps in this deployment guide that use the FortiOS GUI and IPsec wizard is recommended. See Converting FortiGate NGFW to a FortiSASE SPA hub using FortiOS Fabric Overlay Orchestrator on page 10.

FortiSASE points of presence integrate with a hub-and-spoke network using ADVPN as its VPN overlay and BGP for its routing.

This section describes the following configuration settings and the FortiOS GUI configuration steps using the IPsec wizard and additional CLI and GUI configuration that you must configure on your FortiGate NGFW to convert it to a FortiSASE secure private access hub:

- IPsec VPN configuration on page 66
- Tunnel interface configuration on page 70
- Loopback interface configuration on page 71
- Firewall policy configuration on page 72
- BGP configuration on page 74

IPsec VPN configuration

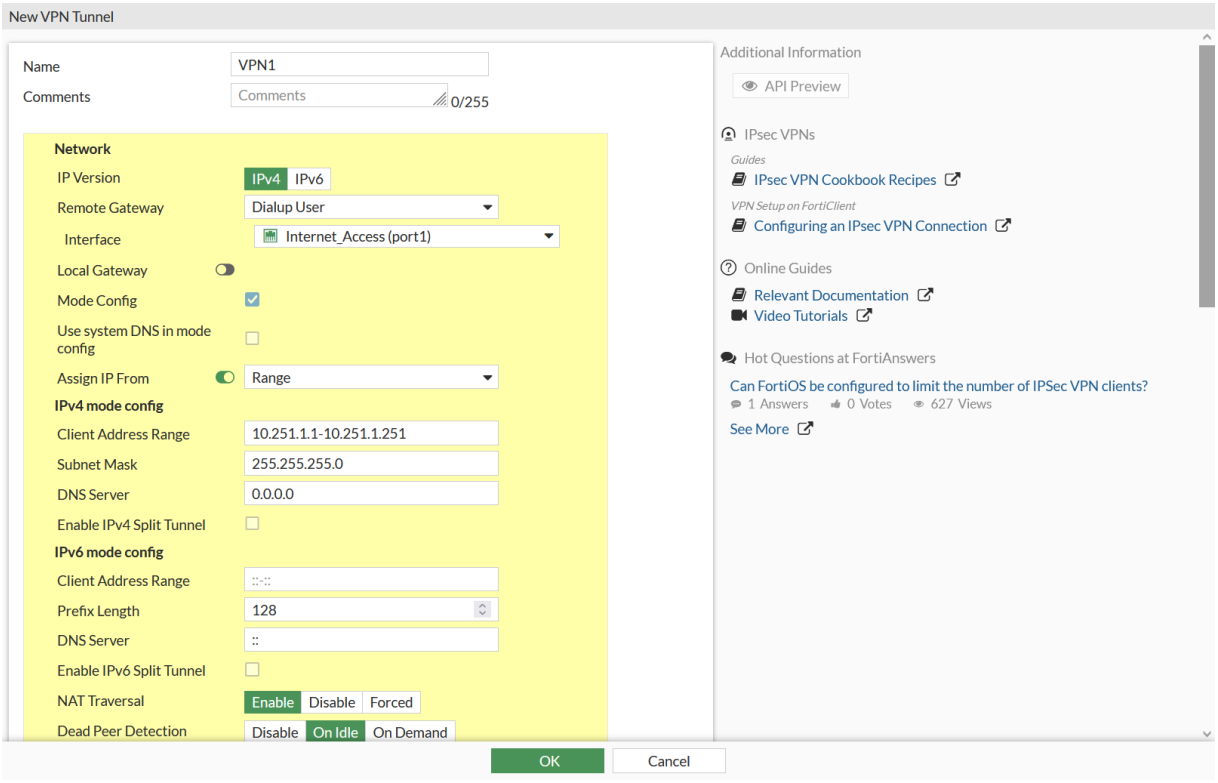
The FortiGate next generation firewall requires the following IPsec VPN settings:

- IKEv2
- Hub configured as an IPsec VPN dialup server. The FortiSASE security points of presence (PoP) act as spokes and connect to your hub via IPsec dialup connections.
- You must enable the mode config setting. Each FortiSASE security PoP acquires IP addresses and automatically configures their tunnel interfaces IP addresses with the acquired IP address. You also use this IP address to set up BGP peering.
- On spokes, remote gateway(s) where one overlay tunnel should be established per underlay even though multiple WAN underlays exist
- Using mode config for dynamic IP address
- Use network overlay IDs for each overlay tunnel configuring `set network-overlay enable` and `set network-id <n>`
- Preshared key for each overlay tunnel
- Phase 1 and 2 proposals and settings
  - For IPsec phase 1, the following proposals are supported:
    aes128-sha256
    aes256-sha256
    aes128-sha1
    aes256-sha1
    DH groups 14 and 5
  - For IPsec phase 2, the following proposals are supported:
    aes128-sha1
    aes256-sha1
    aes128-sha256
    aes256-sha256
    aes128gcm
    aes256gcm
    chacha20poly1305
    DH groups 14 and 5
- Hub configured with `set auto-discovery-sender enable` to enable ADVPN on the hub

The following settings are only examples. Do not consider them as recommended settings.

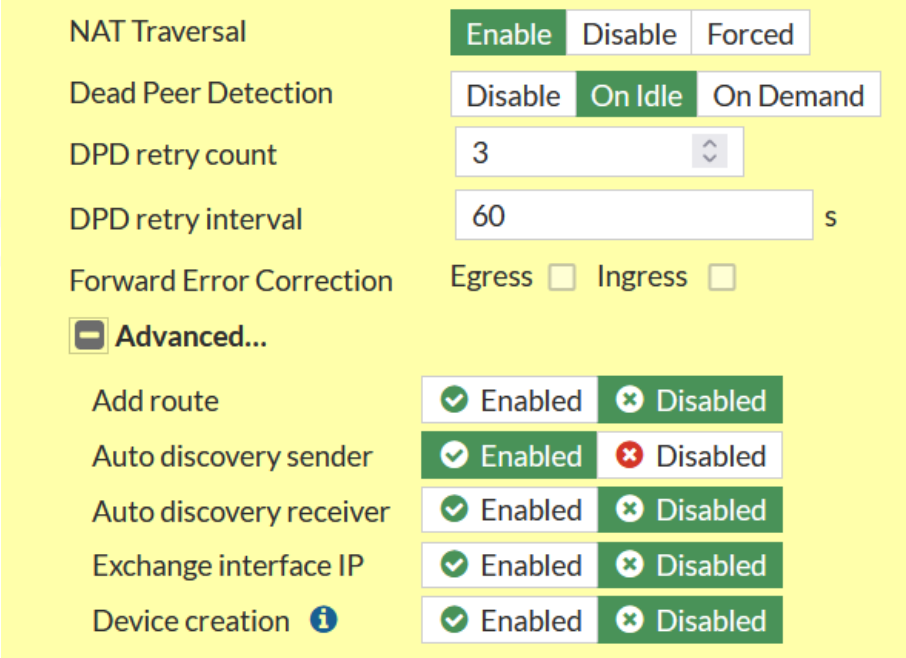
To configure an IPsec VPN tunnel using the GUI:

1. Go to *VPN* > *IPsec Tunnels*.
2. Click *Create New* > *IPsec Tunnel*. The *VPN creation Wizard* displays.
3. Set the following options, then click *Next*:
   a. In the *Name* field, enter VPN1.
   b. For *Template type*, select *Custom*.
4. Set the *Network* options:
   a. For *IP Version*, select *IPv4*.
   b. From the *Remote Gateway* dropdown list, select *Dialup User*.
   c. From the *Interface* dropdown list, select the WAN interface that the hub will listen on for VPN peer connections.
   d. Enable *Mode Config*.
   e. Enable *Assign IP From*, then select *Range* from the dropdown list.
5. Set the *IPv4 mode config* options:
   a. Configure the *Client Address Range*, *Subnet Mask*, and *DNS Server* fields to automate remote client addressing.
   b. Deselect *Enable IPv4 Split Tunnel*.

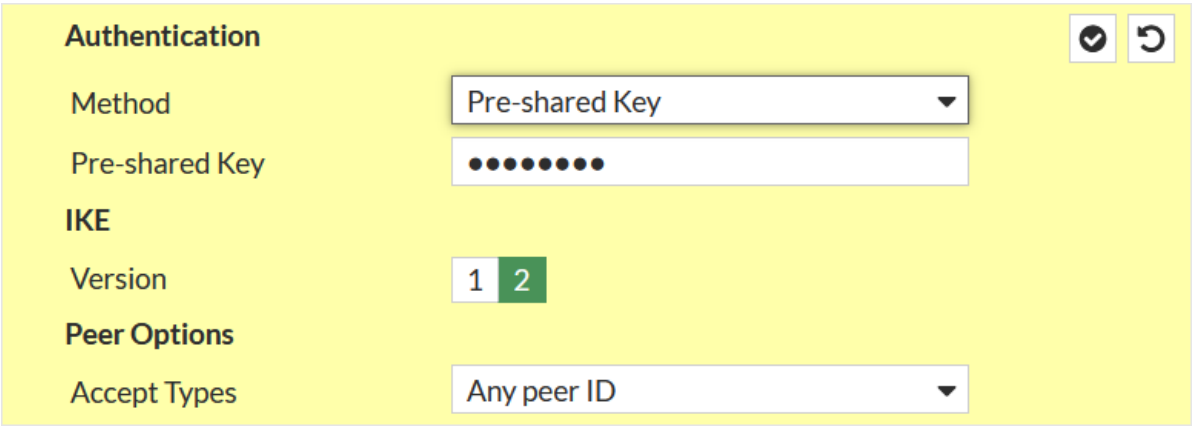


6. Set the remaining *Network* options:
   a. For *NAT Traversal*, select *Enable*.
   b. For *Dead Peer Detection*, select *On Idle*.
   c. In the *DPD retry count* field, enter 3.
   d. In the *DPD retry interval* field, enter 60.
   e. For *Forward Error Correction*, disable *Egress* and *Ingress*.
7. Expand *Advanced*, then set the following options:
   a. For *Add route*, select *Disabled*.
   b. For *Auto discovery sender*, select *Enabled*.

c. For *Auto discovery receiver*, select *Disabled*.
d. For *Exchange interface IP*, select *Disabled*.
e. For *Device creation*, select *Disabled*.



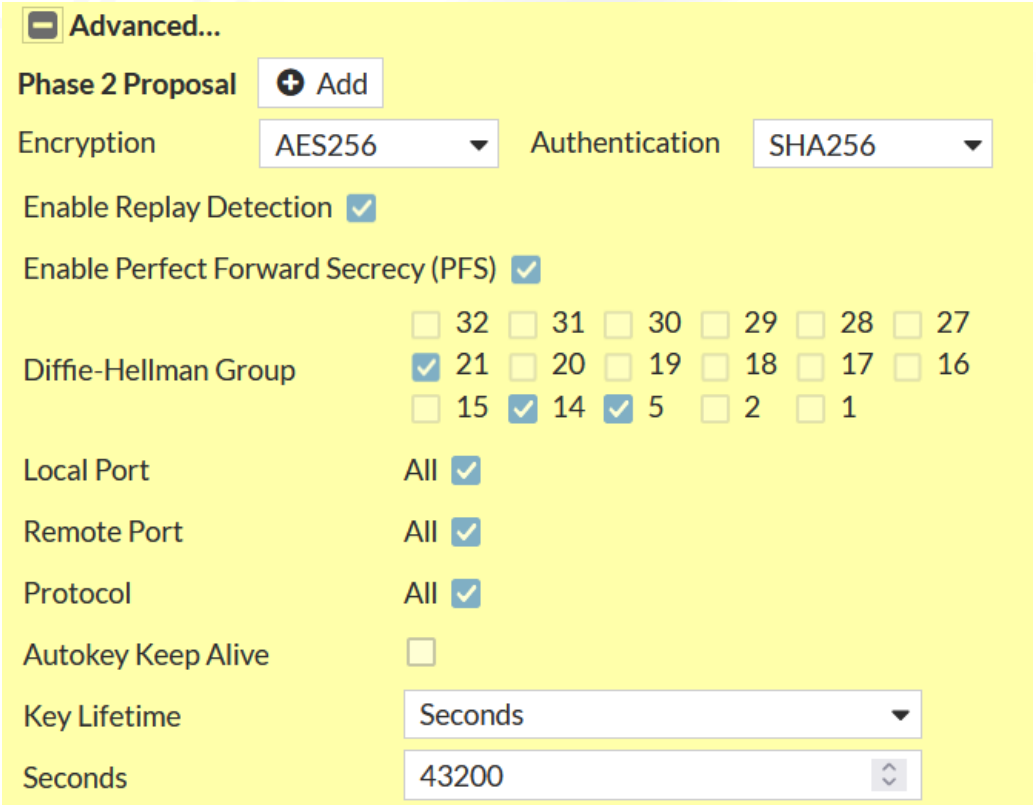
8. Set the *Authentication* options:
   a. From the *Method* dropdown list, select *Pre-shared Key*.
   b. In the *Pre-shared Key* field, enter an alphanumeric string.
   c. For *IKE > Version*, select *2*.
   d. From the *Accept Types* dropdown list, select *Any peer ID*.



9. Set the *Phase 1 Proposal* options:
   a. Add or remove *Encryption* and *Authentication* combinations as desired.
   b. Configure your desired *Diffie-Hellman Groups*, *Key Lifetime*, and *Local ID* (optional).

10. Set the *New Phase 2* options:
    a. If desired, enter a new value in the *Name* field. Otherwise, this defaults to the phase 1 name.
    b. Change the *Local Address* or *Remote Address* as needed. Otherwise, this defaults to 0.0.0.0/0.0.0.0 for both addresses, which is the wildcard subnet, allowing all subnets.

11. Expand *Advanced*, then set the following options:
    a. Add or remove *Encryption* and *Authentication* combinations as desired.
    b. Select *Enable Replay Detection*.
    c. Select *Enable Perfect Forward Secrecy (PFS)*.
    d. Select your desired *Diffie-Hellman Groups*.
    e. For *Local Port*, *Remote Port*, and *Protocol*, select *All*.
    f. Deselect *Autokey Keep Alive*.
    g. From the *Key Lifetime* dropdown list, select *Seconds*.
    h. In the *Seconds* field, enter the desired key lifetime value in seconds.



12. In the CLI, enable network overlays and configure the VPN gateway network ID. Replace VPN1 with the IPsec VPN phase 1 name. Replace 1 with the integer value that corresponds to the network ID. These options are unavailable in the GUI and you must run these CLI commands to configure them:

```
config vpn ipsec phase1-interface
  edit VPN1
    set network-overlay enable
    set network-id 1
  next
end
```

To configure an IPsec VPN tunnel using the CLI:

To allow for dynamic scaling of customer environments, as-needed, it is necessary to use the following mode configuration settings that make use of a /24 subnet for the mode configuration IP address space:

set ipv4-start-ip 192.168.1.1

set ipv4-end-ip 192.168.1.252

set ipv4-netmask 255.255.255.0

Depending on the size of the customer, the mode configuration IP address space may need to be even larger than a /24 subnet.

```
config vpn ipsec phase1-interface
    edit VPN1
        set type dynamic
        set interface port1
        set ike-version 2
        set peertype any
        set net-device disable
        set mode-cfg enable
        set proposal aes256-sha256
        set add-route disable
        set dpd on-idle
        set dhgrp 21 14 5
        set auto-discovery-sender enable
        set network-overlay enable
        set network-id 1
        set ipv4-start-ip 10.251.1.1
        set ipv4-end-ip 10.251.1.252
        set ipv4-netmask 255.255.255.0
        set psksecret < pre-shared key >
        set dpd-retryinterval 60
    next
end
config vpn ipsec phase2-interface
    edit VPN1
        set phase1name VPN1
        set proposal aes256-sha256
    next
end
```

Tunnel interface configuration

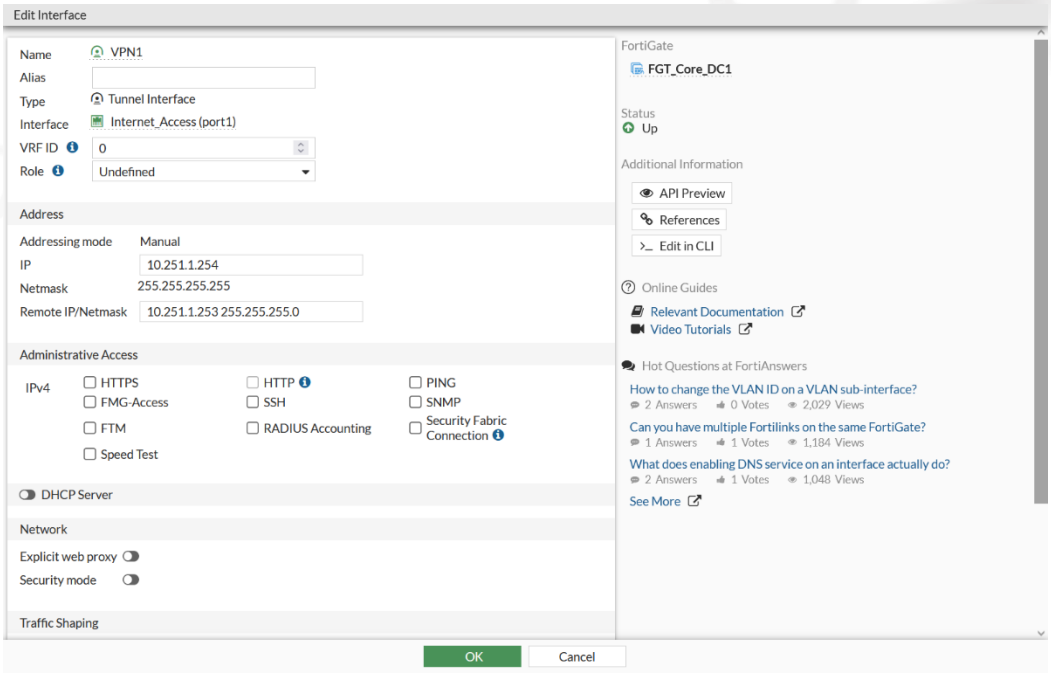
You must assign a static IP address to the tunnel interface. This configuration is required to support BGP peering between the secure private access hub and the FortiSASE security points of presence.

The following settings are only examples. Do not consider them as recommended settings.

To create the tunnel interface using the GUI:

1. Go to *Network* > *Interfaces*.
2. Under *Physical Interface*, expand your WAN interface to display your IPsec VPN tunnel interface. Click the tunnel interface and click *Edit*.

3. In the *Edit Interface* dialog, do the following:
   a. Set the *IP* and *Remote IP/Netmask*.
   b. For *Administrative Access*, select *PING*.
4. Click *OK* to save the changes.



To create the tunnel interface using the CLI:

```
config system interface
    edit "VPN1"
        set vdom "root"
        set ip 10.251.1.254 255.255.255.255
        set allowaccess ping
        set type tunnel
        set remote-ip 10.251.1.253 255.255.255.0
        set interface "port1"
    next
end
```

Loopback interface configuration

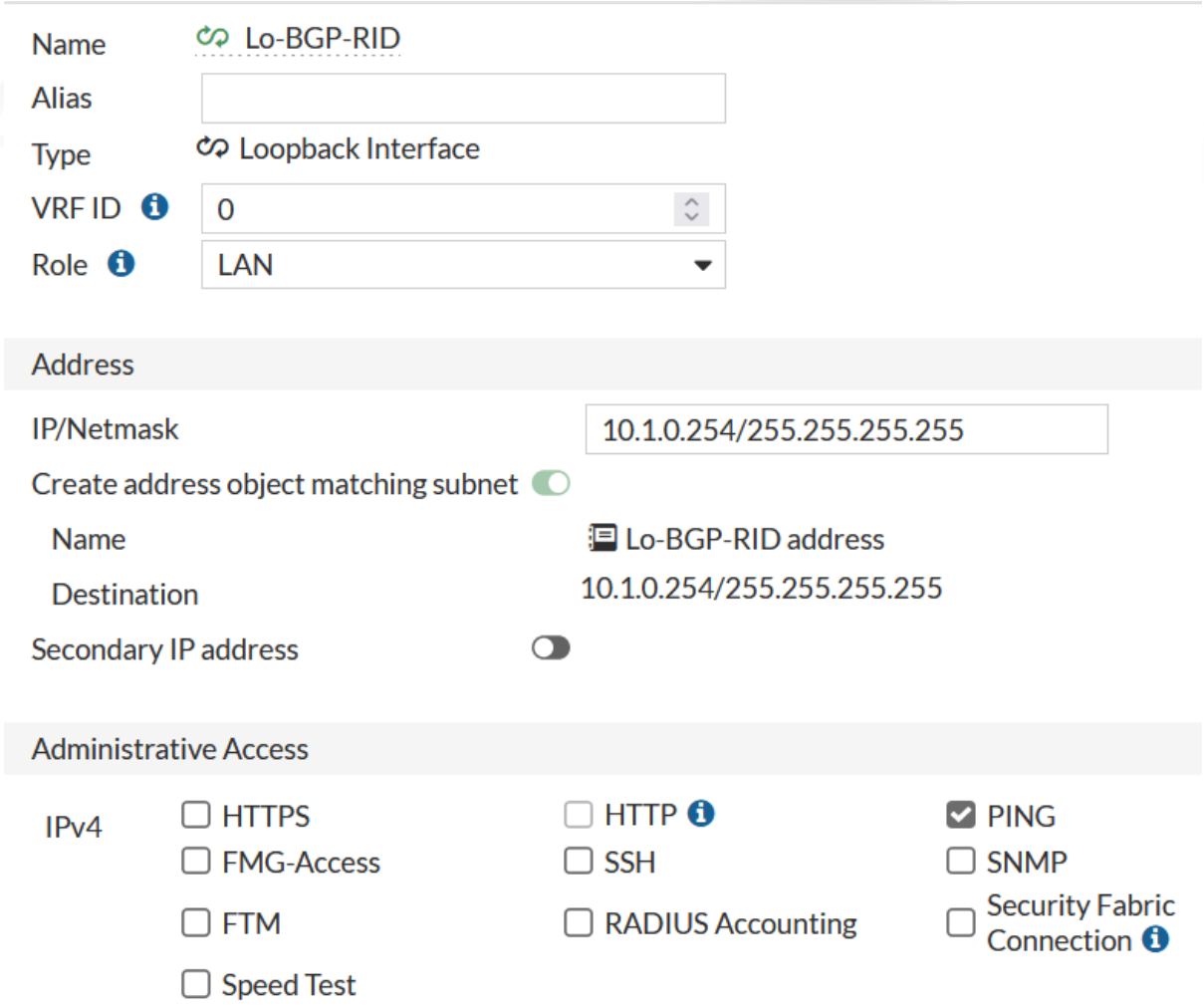
You must create a loopback interface on the FortiGate hub. The configuration uses the loopback interface to establish BGP peering with the FortiSASE security points of presence (PoP) to dynamically learn routes to your environment and provide a health check target for the performance SLA on the FortiSASE security PoPs.

The following settings are only examples. Do not consider them as recommended settings.

To configure the loopback interface using the GUI:

1. Go to *Network* > *Interfaces*.
2. Click *Create New* > *Interface*.

3. Create a new loopback interface using the following settings:
   a. In the *Name* field, enter Lo-BGP-RID.
   b. For *Type*, select *Loopback Interface*.
   c. In the *IP/Netmask* field, enter 10.1.0.254/255.255.255.255.
   d. Under *Administrative Access*, select *PING*.
   e. Click *OK*.



To configure the loopback interface using the CLI:

```
config system interface
    edit "Lo-BGP-RID"
        set vdom "root"
        set ip 10.1.0.254 255.255.255.255
        set allowaccess ping
        set type loopback
    next
end
```

Firewall policy configuration

To allow health checks from FortiSASE security points of presence to access the target SLA, as well as to allow FortiSASE remote users to access protected resources, you must configure these corresponding firewall policies to allow this traffic as this topic demonstrates.

The following settings are only examples. Do not consider them as recommended settings.

To configure firewall policies using the GUI:

1. This deployment requires a spoke-to-hub LAN firewall policy. This policy allows traffic sourced from a spoke subnet destined for hub subnets. Create the policy:
   a. Go to *Policy & Objects* > *Firewall Policy*.
   b. Click *Create New*. The *New Policy* pane displays.
   c. Set the following options:
      i. For *Incoming interface*, select *VPN1*.
      ii. For *Outgoing interface*, select port4.
      iii. For *Source*, select *all*.
      iv. For *Destination*, select *all*.
      v. From the *Schedule* dropdown list, select *always*.
      vi. For *Service*, select *ALL*.
      vii. For *Action*, select *Accept*.
      viii. Disable *NAT*.
      ix. Select *Enable this policy*.
   d. Click *OK*.
2. This deployment requires a spoke-to-spoke firewall firewall policy. This policy allows traffic sourced from a spoke subnet destined for other spoke subnets. Create the policy:
   a. Go to *Policy & Objects* > *Firewall Policy*.
   b. Click *Create New*. The *New Policy* pane displays.
   c. Set the following options:
      i. For *Incoming interface*, select *VPN1*.
      ii. For *Outgoing interface*, select *VPN1*.
      iii. For *Source*, select *all*.
      iv. For *Destination*, select *all*.
      v. From the *Schedule* dropdown list, select *always*.
      vi. For *Service*, select *ALL*.
      vii. For *Action*, select *Accept*.
      viii. Disable *NAT*.
      ix. Select *Enable this policy*.
   d. Click *OK*.
3. Create a spoke-to-loopback firewall policy. This policy allows health check traffic from a spoke to the hub's loopback interface:
   a. Go to *Policy & Objects* > *Firewall Policy* and click *Create New*. The *New Policy* pane displays.
   b. In the *Name* field, enter Lo-HC.
   c. Set the following options:
      i. For *Incoming interface*, select *VPN1*.
      ii. For *Outgoing interface*, select *Lo-BGP-RID*.
      iii. For *Source*, select *all*.
      iv. For *Destination*, select *all*.
      v. From the *Schedule* dropdown list, select *always*.
      vi. For *Service*, select *ALL*.

vii. For *Action*, select *Accept*.
viii. Disable *NAT*.
ix. Select *Enable this policy*.

d. Click *OK* to save changes.

To configure firewall policies using the CLI:

```
config firewall policy
    edit 1
        set name "Spoke-to-Hub"
        set srcintf "VPN1"
        set dstintf "port4"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL”
        set logtraffic all
    next
    edit 2
        set name "Spoke-to-Spoke"
        set srcintf "VPN1"
        set dstintf "VPN1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL”
        set logtraffic all
    next
    edit 3
        set name "Lo-BGP-HC"
        set srcintf "VPN1"
        set dstintf "Lo-BGP-RID"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
end
```

BGP configuration

FortiSASE security points of presence (PoP) connect to the hub FortiGate and establish iBGP peering. FortiSASE security PoPs learn routes to your network but do not advertise any route except their router-id IP address.

The hub FortiGate requires the following BGP settings:

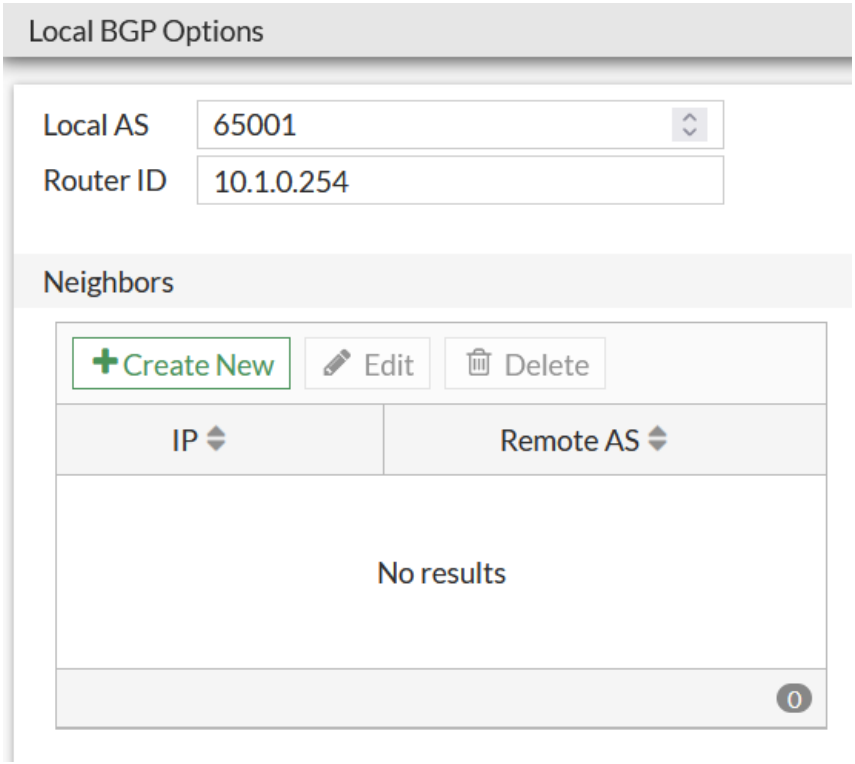
- AS number
- Router ID
- Using iBGP for dynamic routing via overlays
- BGP neighbor IP address for each overlay
- BGP neighbor group configured on the hub to dynamically peer with FortiSASE security PoPs
- One BGP session per overlay between the hub and each FortiSASE security PoP

The following settings are only examples. Do not consider them as recommended settings.

To configure BGP using the GUI:

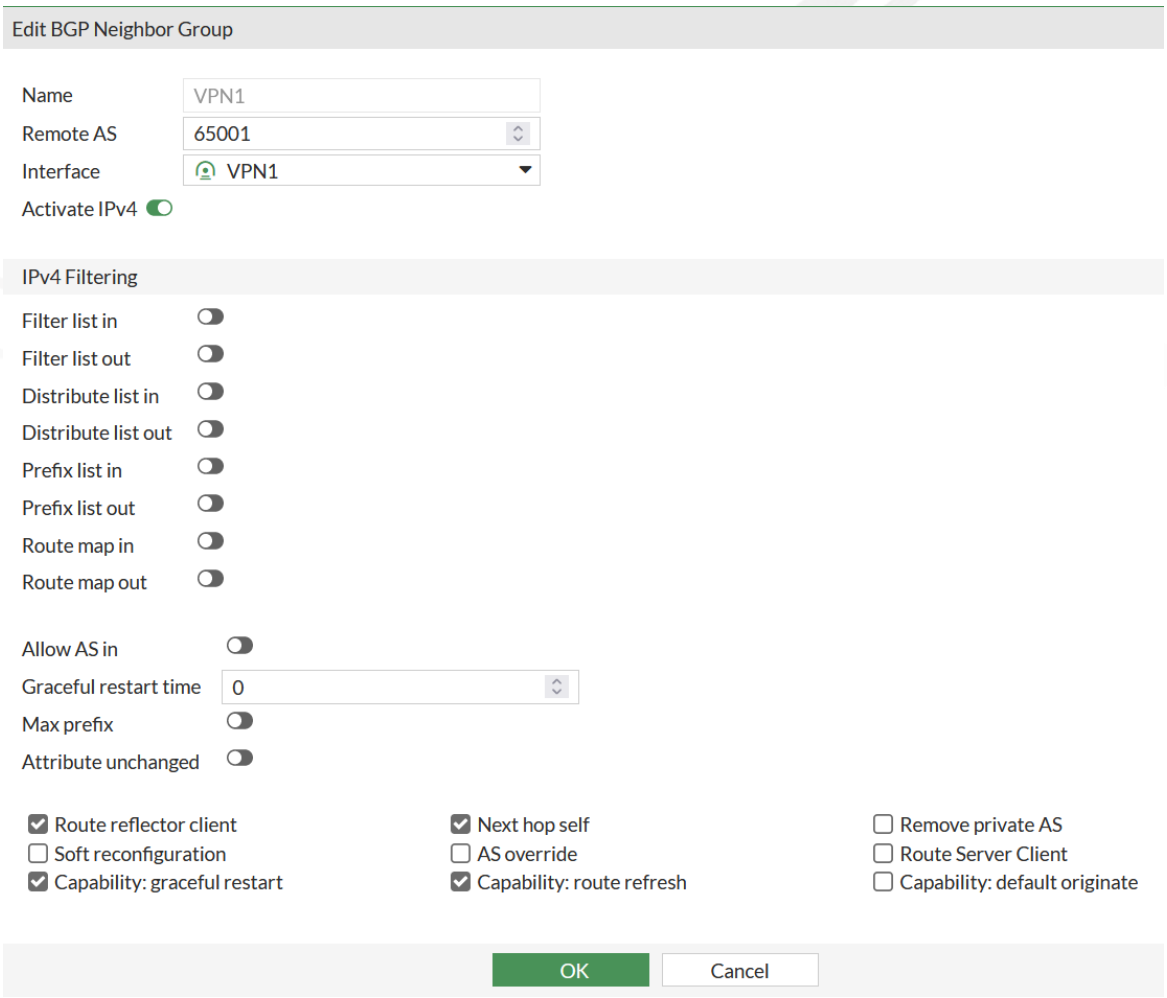
If you cannot view the *Network* > *BGP* tree menu, go to *System* > *Feature Visibility* and enable *Advanced Routing* in the *Core Features* column.

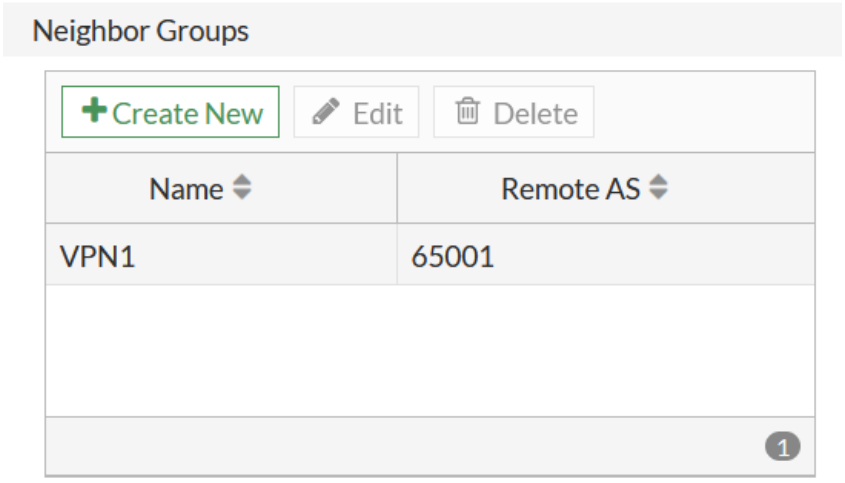
1. Go to *Network* > *BGP*. Confirm that the *Local AS* field is set to 65001.
2. In the *Router ID* field, enter 10.1.0.254, which is the loopback interface IP address.
3. Configure neighbor options:
   a. In *Neighbor Groups*, create a new neighbor group:
      i. Click *Create New*. The *Add BGP Neighbor Group* pane displays.



      ii. In the *Remote AS* field, enter 65001.
      iii. Set *Interface* to the VPN tunnel interface on the hub used to listen to spoke VPN connections. For example, you may select VPN1.
      iv. Enable *Activate IPv4*.
      v. Disable *Attribute unchanged*.
      vi. Select the following options:
         - *Route reflector client*
         - *Next hop self*
         - *Capability: graceful restart*
         - *Capability: route refresh*

vii. Click *OK*.





b. Click *Apply* to perform a hard refresh of the browser.

c. In *Neighbor Ranges*, create a new neighbor range:

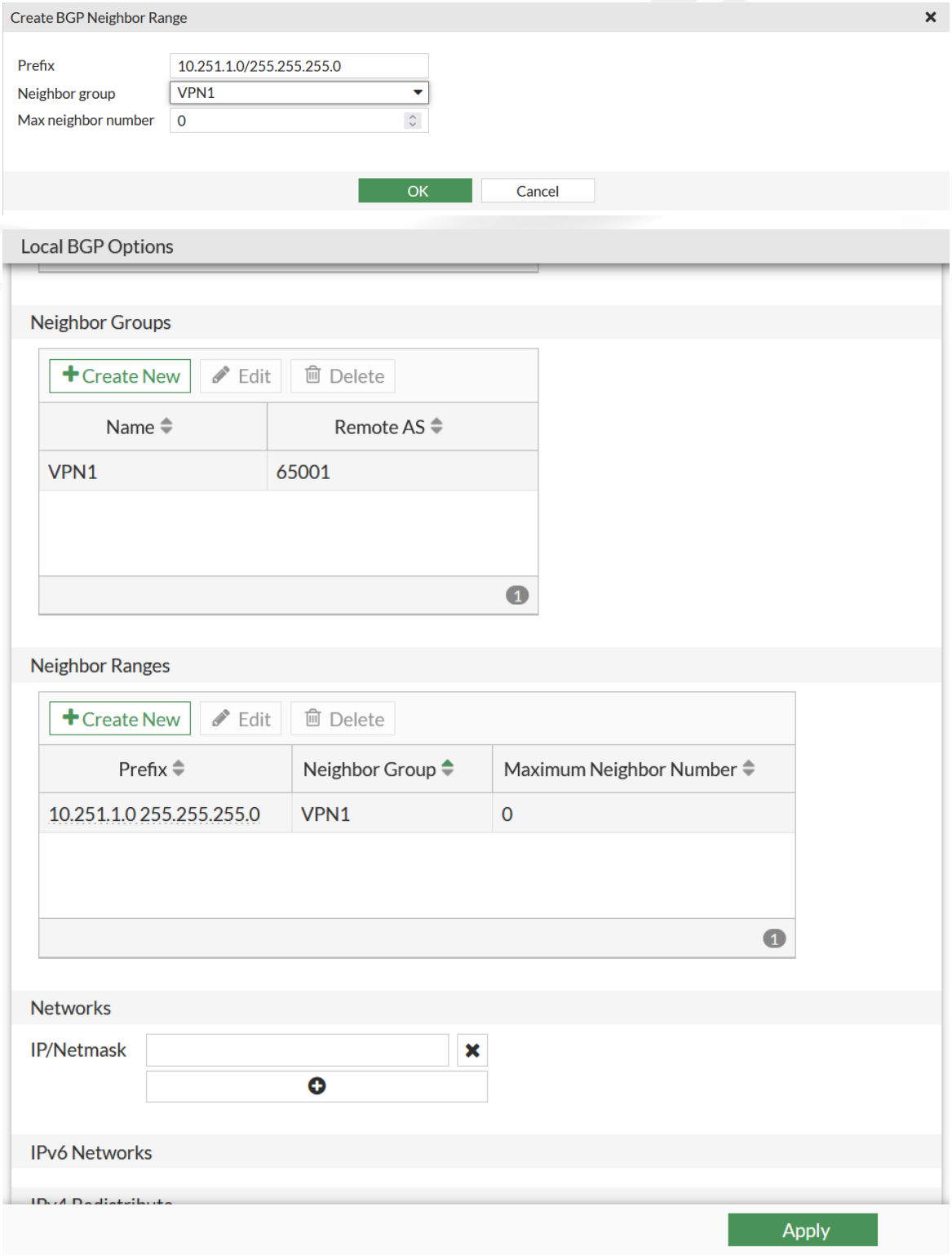
   i. Click *Create New*. The *Create Neighbor Range* pane displays.

   ii. In the *Prefix* field, enter 10.251.1.0/255.255.255.0, which is the VPN peers subnet assigned using mode config.

   iii. From the *Neighbor group* dropdown list, select *VPN1*.

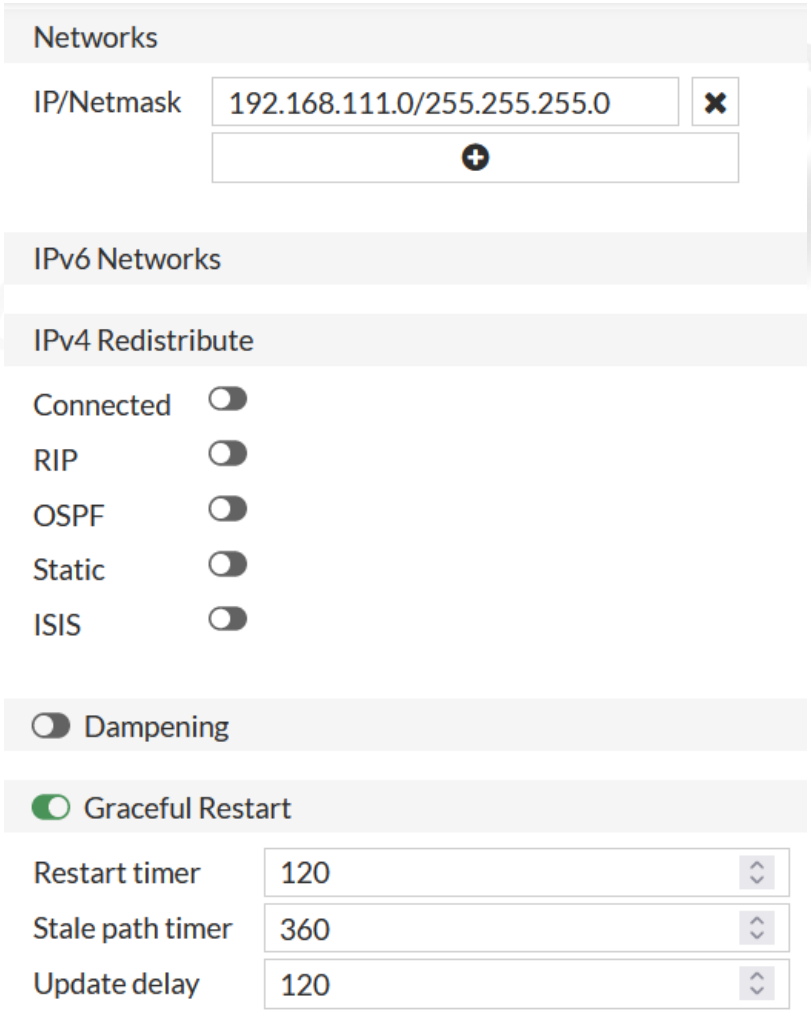
   iv. In the *Max neighbor number* field, enter 0.

v. Click *OK*.

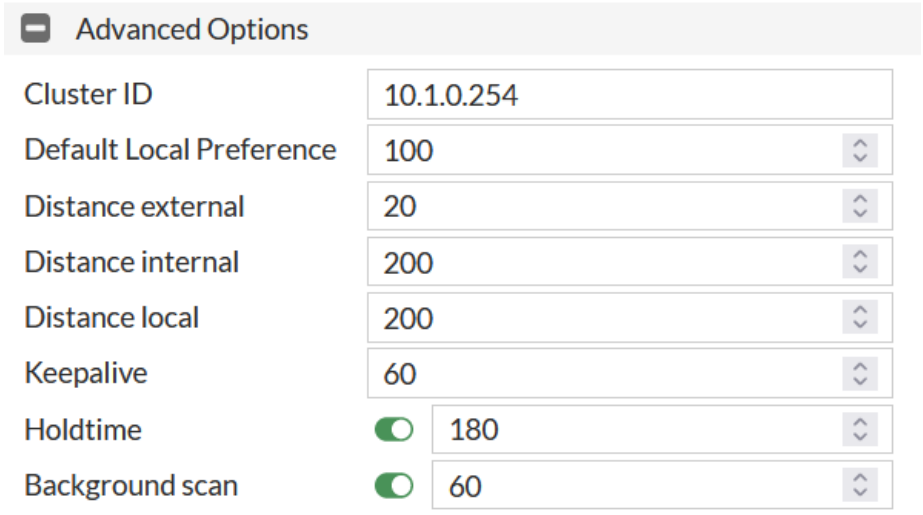


4. In *Networks*, in the *IP/Netmask* field, enter 192.168.111.0 255.255.255.0.
5. Enable *Graceful Restart* and configure the following options:
   a. In the *Restart timer* field, enter 120.
   b. In the *Stale path timer* field, enter 360.

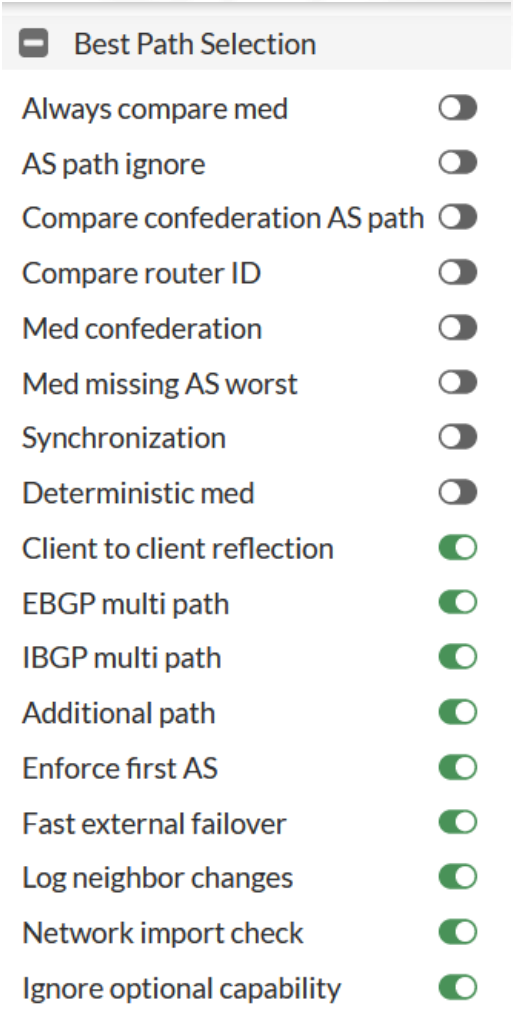
c. In the *Update delay* field, enter 120.



6. Under *Advanced Options*, configure the following:
   a. In the *Keepalive* field, enter 60.
   b. Enable *Holdtime* and enter 180.
   c. Enable *Background scan* and enter 60.



7. Under *Best Path Selection*, enable the following options:
   a. *Client to client reflection*
   b. *EBGP multi path*
   c. *IBGP multi path*
   d. *Additional path*
   e. *Enforce first AS*
   f. *Fast external failover*
   g. *Log neighbor changes*
   h. *Network import check*
   i. *Ignore optional capability*



8. Click *Apply*.
9. Configure the following CLI options. These options are not available in the GUI and you must run these CLI commands to configure them:

```
config router bgp
  config neighbor-group
       edit "VPN1"
           set link-down-failover enable
           set additional-path both
           set adv-additional-path 4
       next
```

```
        end
    end
```

To configure BGP using the CLI:

```
config router bgp
    set as 65001
    set ibgp-multipath enable
    set additional-path enable
    set graceful-restart enable
    set additional-path-select 4
    config neighbor-group
        edit "VPN1"
            set capability-graceful-restart enable
            set link-down-failover enable
            set next-hop-self enable
            set remote-as 65001
            set additional-path both
            set adv-additional-path 4
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.251.1.0 255.255.255.0
            set neighbor-group "VPN1"
        next
    end
end
```

www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

72-252-1125851-20250520